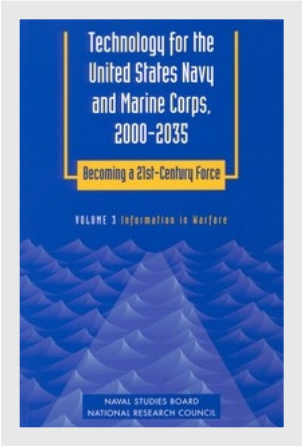

Technology for the United States Navy and Marine Corps, 2000-2035 Becoming a 21st-Century Force: Volume 3: Information in Warfare

DETAILS

144 pages | 6 x 9 | PAPERBACK
ISBN 978-0-309-05898-8 | DOI 10.17226/5864

AUTHORS

Committee on Technology for Future Naval Forces, National Research Council

Technology for the United States Navy and Marine Corps, 2000-2035

Becoming a 21st-Century Force

VOLUME 3 Information in Warfare

Panel on Information in Warfare
Committee on Technology for Future Naval Forces
Naval Studies Board
Commission on Physical Sciences, Mathematics, and Applications
National Research Council

NATIONAL ACADEMY PRESS
Washington, D.C. 1997

NOTICE: The project that is the subject of this report was approved by the Governing Board of the National Research Council, whose members are drawn from the councils of the National Academy of Sciences, the National Academy of Engineering, and the Institute of Medicine. The members of the committee responsible for the report were chosen for their special competences and with regard for appropriate balance.

This report has been reviewed by a group other than the authors according to procedures approved by a Report Review Committee consisting of members of the National Academy of Sciences, the National Academy of Engineering, and the Institute of Medicine.

The National Academy of Sciences is a private, nonprofit, self-perpetuating society of distinguished scholars engaged in scientific and engineering research, dedicated to the furtherance of science and technology and to their use for the general welfare. Upon the authority of the charter granted to it by the Congress in 1863, the Academy has a mandate that requires it to advise the federal government on scientific and technical matters. Dr. Bruce Alberts is president of the National Academy of Sciences.

The National Academy of Engineering was established in 1964, under the charter of the National Academy of Sciences, as a parallel organization of outstanding engineers. It is autonomous in its administration and in the selection of its members, sharing with the National Academy of Sciences the responsibility for advising the federal government. The National Academy of Engineering also sponsors engineering programs aimed at meeting national needs, encourages education and research, and recognizes the superior achievements of engineers. Dr. William A. Wulf is president of the National Academy of Engineering.

The Institute of Medicine was established in 1970 by the National Academy of Sciences to secure the services of eminent members of appropriate professions in the examination of policy matters pertaining to the health of the public. The Institute acts under the responsibility given to the National Academy of Sciences by its congressional charter to be an adviser to the federal government and, upon its own initiative, to identify issues of medical care, research, and education. Dr. Kenneth I. Shine is president of the Institute of Medicine.

The National Research Council was organized by the National Academy of Sciences in 1916 to associate the broad community of science and technology with the Academy's purposes of furthering knowledge and advising the federal government. Functioning in accordance with general policies determined by the Academy, the Council has become the principal operating agency of both the National Academy of Sciences and the National Academy of Engineering in providing services to the government, the public, and the scientific and engineering communities. The Council is administered jointly by both Academies and the Institute of Medicine. Dr. Bruce Alberts and Dr. William A. Wulf are chairman and vice chairman, respectively, of the National Research Council.

This work was performed under Department of the Navy Contract N00014-96-D-0169/0001 issued by the Office of Naval Research under contract authority NR 201-124. However, the content does not necessarily reflect the position or the policy of the Department of the Navy or the government, and no official endorsement should be inferred.

Copies available from:

Naval Studies Board
National Research Council
2101 Constitution Avenue, N.W.
Washington, D.C. 20418

Printed in the United States of America

PANEL ON INFORMATION IN WARFARE

VINCENT VITTO, Lincoln Laboratory, Massachusetts Institute of Technology, *Chair*
PHILIP S. ANSELMO, Northrop Grumman Corporation, *Vice Chair*
NORVAL L. BROOME, Mitre Corporation
J. ROBERT COLLINS, E Systems
BURTON I. EDELSON, George Washington University
JOHN F. EGAN, Lockheed Martin Corporation
ROBERT HUMMEL, Courant Institute of Mathematical Sciences, New York University
GERALD McNIFF, Northrop Grumman Corporation
ROBERT NESBIT, Mitre Corporation
STANLEY R. ROBINSON, Environmental Research Institute of Michigan
JULIE JCH RYAN, Booz, Allen and Hamilton
H. GREGORY TORNATORE, Applied Physics Laboratory, Johns Hopkins University
BRUCE WALD, Center for Naval Analyses
MARY LETICIA VAJTA-WILLIAMS, Space Imaging, Inc.

Navy Liaison Representatives

LCDR HARRY COKER, USN, Department of Defense Space Architect
CAPT MATTHEW ROGERS, USN, Department of Defense Space Architect
LtCol FRANK WALIZER, USMC, Office of the Chief of Naval Operations, N853H
CAPT MICHAEL WINSLOW, USN, Office of the Chief of Naval Operations, N6C

Consultants

LEE M. HUNT
SIDNEY G. REED, JR.
JAMES G. WILSON

Staff

RONALD D. TAYLOR, Director, Naval Studies Board
PETER W. ROONEY, Program Officer
SUSAN G. CAMPBELL, Administrative Assistant
MARY G. GORDON, Information Officer
CHRISTOPHER A. HANNA, Project Assistant

COMMITTEE ON TECHNOLOGY FOR FUTURE NAVAL FORCES

DAVID R. HEEBNER, Science Applications International Corporation (retired), Study Director
ALBERT J. BACIOCCO, JR., The Baciocco Group, Inc.
ALAN BERMAN, Applied Research Laboratory, Pennsylvania State University
NORMAN E. BETAQUE, Logistics Management Institute
GERALD A. CANN, Raytheon Company
GEORGE F. CARRIER, Harvard University
SEYMOUR J. DEITCHMAN, Institute for Defense Analyses (retired)
ALEXANDER FLAX, Potomac, Maryland
WILLIAM J. MORAN, Redwood City, California
ROBERT J. MURRAY, Center for Naval Analyses
ROBERT B. OAKLEY, National Defense University
JOSEPH B. REAGAN, Saratoga, California
VINCENT VITTO, Lincoln Laboratory, Massachusetts Institute of Technology

Navy Liaison Representatives

RADM JOHN W. CRAINE, JR., USN, Office of the Chief of Naval Operations, N81 (as of July 4, 1996)
VADM THOMAS B. FARGO, USN, Office of the Chief of Naval Operations, N81 (through July 3, 1996)
RADM RICHARD A. RIDDELL, USN, Office of the Chief of Naval Operations, N91
CDR DOUGLASS BIESEL, USN, Office of the Chief of Naval Operations, N812C1
PAUL G. BLATCH, Office of the Chief of Naval Operations, N911E

Marine Corps Liaison Representative

LtGen PAUL K. VAN RIPER, USMC, Marine Corps Combat Development Command

Consultants

LEE M. HUNT
SIDNEY G. REED, JR.
JAMES G. WILSON

Staff

RONALD D. TAYLOR, Director, Naval Studies Board
PETER W. ROONEY, Program Officer
SUSAN G. CAMPBELL, Administrative Assistant
MARY G. GORDON, Information Officer
CHRISTOPHER A. HANNA, Project Assistant

NAVAL STUDIES BOARD

Navy Liaison Representatives

Marine Corps Liaison Representative

LtGen PAUL K. VAN RIPER, USMC, Marine Corps Combat Development Command

RONALD D. TAYLOR, Director
PETER W. ROONEY, Program Officer
SUSAN G. CAMPBELL, Administrative Assistant
MARY G. GORDON, Information Officer
CHRISTOPHER A. HANNA, Project Assistant

COMMISSION ON PHYSICAL SCIENCES, MATHEMATICS, AND APPLICATIONS

Preface

This report is part of the nine-volume series entitled *Technology for the United States Navy and Marine Corps, 2000-2035: Becoming a 21st-Century Force*. The series is the product of an 18-month study requested by the Chief of Naval Operations (CNO). To carry out this study, eight technical panels were organized under the Committee on Technology for Future Naval Forces to examine all of the specific technical areas called out in the terms of reference.

On November 28, 1995, the Chief of Naval Operations requested that the National Research Council initiate (through its Naval Studies Board) a thorough examination of the impact of advancing technology on the form and capability of the naval forces to the year 2035. The terms of reference of the study specifically asked for an identification of "present and emerging technologies that relate to the full breadth of Navy and Marine Corps mission capabilities," with specific attention to "(1) information warfare, electronic warfare, and the use of surveillance assets; (2) mine warfare and submarine warfare; (3) Navy and Marine Corps weaponry in the context of effectiveness on target; [and] (4) issues in caring for and maximizing effectiveness of Navy and Marine Corps human resources." Ten specific technical areas were identified to which attention should be broadly directed. The CNO's letter of request with the full terms of reference is given in Appendix A of this report.

The Panel on Information in Warfare was constituted to address the information aspects of the terms of reference. As part of its effort, particular attention was to be directed to item 2: "Information warfare, electronic warfare and the exploitation of surveillance assets, both through military and commercial developments, should receive special attention in the review. The efforts should

concentrate on information warfare, especially defensive measures that affordably provide the best capability." However, it must be acknowledged that information touches broadly on many aspects of Navy and Marine Corps capabilities beyond just the issues mentioned above. The panel accepted as its charge a study of the broader implications of information in warfare.

Panel membership included expertise in command, control, communications, computing, intelligence (C^4I), electronic warfare, information warfare, telecommunications, naval communications, systems engineering, surveillance systems, targeting systems, image processing, signal processing, data automation, computer security, computer engineering, satellite communications, space technologies, radar, electronic countermeasures, modeling and simulation, computer science, and imaging sensors.

To carry out its task, the panel met eight times for a total of 15 days to receive briefings from Service and industry representatives, visit facilities, deliberate, and draft its report. In addition, the panel participated in the three plenary meetings for the overall study. The first, in March 1996, was addressed by the Chief of Naval Operations and many high-level officials of the Navy Department, the other Services, the Defense Department, and industry. This served as an organization meeting and conveyed a common, starting information base to the entire study membership. At the second plenary session, in October 1996, all the members of the study had their first opportunity to review each other's work, to see how the results of all the panels' work were coming together into an integrated message, and to feed the results back into their own efforts. The third plenary session, in March 1997, served as a coordination and writing session in which all of the panels' reports and the overview report were completed for final review. The panel chair and vice chair also participated in bimonthly meetings of the Committee on Technology for Future Naval Forces. These meetings served to inform the panel chairs and study leadership of progress in the individual panels' efforts, and to resolve issues that cut across the responsibilities of more than one panel. The meetings also helped to ensure that common attention was paid to the relationships of the diverse panel outputs to each other and the significance of those outputs for the naval forces. A total of some 40 days was encompassed in meetings by the panel and its chair. The panel's report emphasizes the significance of and critical dependence on information technologies and systems for future naval forces and points toward a direction for achieving information superiority in the future.

Contents

Executive Summary

Future warfare strategies will depend on forward-deployed, dynamic naval forces to execute a broad set of military missions. These missions will range from early, rapid power projection to deter aggression and sustained operations within a joint force structure in a major regional conflict at one end of the spectrum, to special operations activities and humanitarian relief at the other end. These forces are now and will continue to be highly dependent on a wide range of tactical information and subsequently on the supporting information infrastructure. Future naval warfighting strategies are being shaped by trends we see emerging today, particularly within the commercial information services industries worldwide. Naval forces, because of their forward-deployed nature, are critically dependent on timely long-haul information transport and utilization and have been the major user of space systems, particularly satellite communications. The evolution of information and networking services and technologies within the commercial sector and the continued expansion of those services globally will continue with ever-increasing capabilities into the 21st century. By 2035, we will see a world dominated by the proliferation of primarily digital commercial information systems that will provide a broad range of services anywhere in the world. These services will be available to forward-deployed naval forces but likely will also be available to our adversaries. A major challenge for the Department of Defense (DOD) and the Department of the Navy will be the development of strategies and organizational structures to allow for the maximum utilization of global commercially developed information systems while at the same time protecting these critical capabilities from denial or attack and developing the means to deny the use of these systems and services to our adversaries.

To that end, the Department of the Navy must develop a strategy to achieve and maintain *information superiority* for naval forces. Information superiority must be established as a warfare area under an integrated organizational structure with responsibility for resource planning, program development, and budgeting for all Navy and Marine Corps information systems and services that are not unique to individual platforms or weapons systems. An information-in-warfare system for achieving information superiority comprises:

- Information sources, communications systems, information processing and fusion systems, and decision support and display systems, all seamlessly integrated by an infrastructure;
- The means for protecting these information systems and services by making them diverse, secure, and robust to attack or countermeasures; and
- The means to deny hostile forces the ability to degrade, disrupt, and/or utilize these information systems.

Today these three components are pursued separately and with unequal emphasis. The Department of the Navy must establish an organizational structure that integrates the development, protection, and denial of information services across all naval platforms in a "system of systems" context. The importance of maintaining a tight coupling between information sources, systems, and services to include intelligence, sensors, MCG (mapping, charting, geodesy), command and control, weapons, and targeting systems cannot be overemphasized. We are rapidly moving into an information-rich era involving highly mobile forces, precision-guided weapons, exquisite global situation awareness, focused logistics, and full-dimensional protection of our forces. Information superiority must be the centerpiece for any vision of joint and coalition force operations in the 21st century. Information superiority will not, however, be viewed with the importance it demands unless naval officers are rewarded, career paths established, and education programs put in place within this warfare area.

INFORMATION INFRASTRUCTURE

To establish information superiority, a robust, seamless information infrastructure must be established to allow future military forces to transmit and receive needed information from any point on the globe in a flexible, reconfigurable structure capable of rapidly adapting to changing tactical environments. This information infrastructure must support these needs, while allowing force structures of arbitrary composition to be rapidly formed and fielded. Furthermore, the infrastructure must adapt to varying demands (i.e., surge conditions) during crises and stress imposed by evolving political and military situations. The infrastructure must allow information to be distributed to and from various force elements at any time; its architecture must not be constrained to support a

force-structure hierarchy conceived a priori. Most importantly, the information and services provided to an end user through the infrastructure must be tailored to the user's needs and be relevant to the user's mission, without requiring people at the user's location to sort through volumes of data or images. An information infrastructure meets the warfighter's needs by:

- Providing robust and reliable service;
- Avoiding exposing the user to detection and targeting; and
- Supporting force structures of arbitrary composition by:
  —Moving information in any format from any source to any destination, and
  —Providing information tailored to users' needs.

Commercial interests will continue to drive the development of most information technologies, and the Navy must be prepared to accommodate rapid changes in the direction that commercial capabilities evolve by adopting commercial technologies and equipment and adapting naval practices and systems to incorporate them. Although many developers of military information systems claim that they are using commercial off-the-shelf (COTS) products, closer inspection often reveals that in fact they have modified the commercial product. This practice is markedly less desirable than adopting the product directly without change, because in modifying products the user loses future commercial support for the product, including the ability to insert commercial upgrades, and may end up with the burden of maintaining the system. In particular, because of the utilization of satellite communications to provide connectivity to forward-deployed naval forces, special emphasis must be given to the seamless integration of terrestrial fiber, satellite communications, and in-theater wireless tactical networks. Integration of these diverse, largely commercially developed communications systems into a robust, protected information infrastructure is a critical issue that will require significant Navy Department interest and research and development investment.

INFORMATION CONTENT

Establishing a robust, secure information infrastructure will allow the timely transport of critical information to naval forces deployed worldwide. Of equal importance are the content of the information transported over the infrastructure and the applications that make use of that information. It is important to regard the information content conveyed to the warfighter at any level of command as the end product of a system that is integral to the security of the nation. Indeed, the panel views the information system, consisting of the infrastructure, the information itself, and the processing of that information that transforms the data into meaningful representations, as an essential asset in the repertoire of offensive and defensive systems, on a par with platforms and weapons.

Three aspects of information that affect the value and utility of information content include:

- Sources of information, including DOD, government agencies, commercial, and public-domain sources such as Internet traffic, afforded by an increasingly information-centered society;
- Applications of information for naval activities, organized according to areas of coverage and requirements for timeliness; and
- Processing of information, which is required to transform information into forms that are useful for the corresponding applications. The panel particularly considered processing requirements for two classes of applications: automatic target recognition applications and data fusion applications for information understanding.

An essential aspect of information is its representation. How information is presented, whether to a human or to an automatic analysis system, very much influences the utility of the information. Further, a database can take on new significance when organized in useful ways or when the information is combined with prior statistical observations, as in collaborative filtering. Processing of information can be the vital ingredient in making the information have value. The panel believes that achieving "information understanding" requires the ability to extract useful representations, based on recognition of patterns and fusion of information according to meaningful associations.

The Department of the Navy must support technology development within the domain of information content, including information understanding and recognition theory, where unique military applications are involved. Technologies for improving information content involve information representation, search, integrity, and reasoning, as well as issues associated with information presentation and human performance prediction models. While much of this research and development will be critical to the entire DOD, the Navy Department should play a central and significant leading role in establishing programs in this area, given that forward-deployed naval forces are so information dependent and potentially bandwidth limited. These are not topics that will be dominated by commercial interests, although there are clearly areas of overlap within the global financial, medical, and information systems markets.

SENSORS

Critical to information content are the sensor systems that will provide the basis for situation awareness. Advanced sensor technology is a crucial element for the collection of information. One example of an evolving commercial business area with obvious military applications is airborne and particularly space-based collection of images. In the near term, new ventures in this area will offer afford-

able submeter-resolution panchromatic as well as artificially colorized imagery of most areas of Earth, from commercially launched space platforms. In addition to services and products, this industry will drive the development of low-cost, lightweight advanced sensors that will have spin-offs for uniquely military applications.

In spite of the major contributions the commercial sector is likely to make toward satisfying future military sensor requirements, there will always be a subset of those requirements that has no identifiable, profitable commercial counterpart. Many of the significant radar, electro-optical, and acoustic sensor technologies that will be critical for future military operations will require Navy Department investment to ensure their robust development and tailoring to naval applications. Reconnaissance and surveillance platforms under the control of the joint task force commander will provide some of the information necessary to conduct naval missions and operations. The Navy must ensure that it provides connectivity to those assets provided by other Services or the National[1] community, and it must invest in organic sensors and platforms to meet unique Navy requirements that will not otherwise be satisfied.

INFORMATION WARFARE

Given the critical importance of information to every aspect of naval operations, the area of information security is of concern. The Department of the Navy must be assured of the availability and integrity of both the information infrastructure and information content. Additionally, the Navy Department must be able to create and maintain confidentiality as required. These requirements are complicated by the naval forces' increasing dependencies on and interconnectivities with public and commercial information sources and infrastructure elements. The commercial aspects of the Navy Department's information environment must not prevent the effective exploitation and protection of the information infrastructure or content. The information infrastructure, the sensors that provide data for critical databases, and the information processing systems that will provide the information understanding to support warfighting activities must be protected. The Department of the Navy must also develop the means (including, for example, offensive technologies and infrastructure weapons) to deny U.S. adversaries the information they need.

ATTAINING INFORMATION SUPERIORITY

In conclusion, the Department of the Navy must recognize the significance and critical importance of information technologies and systems for future naval

[1] The term "National" refers to those systems, resources, and assets controlled by the United States government, but not limited to the Department of Defense (DOD).

forces and elevate *information superiority* to a warfare area. The panel recommends that the Department of the Navy:

1. Establish and treat *information superiority* as a warfare area. Provide a mechanism for coordinating all Navy Department command, control, communications, computing, intelligence, surveillance, and reconnaissance (C^4ISR) resources, requirements, and planning, giving due consideration to the evolving missions for naval forces and to current and future capabilities of ISR performed by other Services and agencies. If established, such an area could greatly enhance the capability of joint operations with other services.

2. Encourage information superiority careers. Educate all officers, regular and reserve, about information technologies, resources, and systems needed to support future Navy and Marine Corps operations; define a cadre of specialists; and identify a career path to flag/general officer rank.

3. Adopt commercial information technology, systems, and services wherever possible. Develop technologies only for special Navy and Marine Corps needs such as low-probability-of-intercept communications and connectivity to submerged platforms.

4. Modernize information systems and services aggressively. Strive to involve operational users, research commands, and acquisition organizations in a cohesive relationship that allows the continued rapid insertion of advanced information systems for use by Navy and Marine Corps forces.

5. Focus information infrastructure R&D. Make integration of diverse commercial services and DOD-unique links a primary focus of information infrastructure and network research and development.

6. Manage data sources. Establish a clear policy designating responsibility in the Navy Department for identifying, organizing, classifying, and assuring all relevant information sources that permit information extraction and communication from multiple remote locations. Invest in research on and development of tools and techniques to facilitate this shared information environment.

7. Extract relevant information and knowledge. Adopt commercial data-mining technology for naval applications and pursue a theory of information understanding and apply it to target recognition.

8. Exploit commercial sensing. Consider commercial space-based imaging systems and tools for exploiting them, as well as mechanisms for distributing data, in support of naval applications.

9. Exploit National and joint sensors. Provide online/direct connectivity to naval platforms and Marine Corps units to support long-range and precision-guided munitions.

10. Make information warfare operational. Integrate defense and offense and develop needed technology, systems, tactics, tools, and intelligence support.

1

Impact of Information Technology on Future Naval Forces and Missions

INTRODUCTION

Information and information technologies will so profoundly influence future naval forces and missions that the pursuit of *information superiority* will become a paramount goal in force planning, acquisition, training and education, and operations. Commercial interests have been the primary cause for the dramatic improvement in and rapid growth of the capabilities of information systems, and this trend is expected to continue. The Department of the Navy can leverage these technologies to attain military superiority through information superiority by applying them not only to battle management but also to preparation, planning, and logistics.

In this chapter, the Panel on Information in Warfare discusses information requirements and how current and future technologies can support these requirements. Subsequent chapters focus on the information infrastructure, information content, sensors, and information warfare, and on an action plan for attaining and maintaining *information superiority*.

NAVAL FORCES COMMAND AND CONTROL

The Joint Chiefs of Staff (JCS) define command and control (C^2) as the "exercise of authority and direction by a properly designated commander over assigned forces in the accomplishment of his mission." C^2 functions are performed through an arrangement of personnel, equipment, facilities, and procedures that are employed by a commander in planning, directing, coordinating,

and controlling these forces. This arrangement is often referred to as a command, control, and communications (C^3) system as it embodies functional capabilities that provide tactical pictures of the battle space and communications connectivity. At the center of this system is a complete, accurate, and timely information set on which the commander and his staff base their decisions.

It is easy to see that such functions extend to virtually all echelons of command, from the National Command Authority (NCA) and commander-in-chief (theater and functional) levels down to the individual fighting unit. The availability of timely, accurate, and complete information on all aspects of the projected battle space is a key element in the success of the commander's mission. Information, then, can be considered to be a critical driver of warfare and will significantly influence how warfare will be conducted. Information warfare (IW) has recently become an important element of Department of Defense (DOD) and Navy Department planning and is generally defined as those actions taken to protect one's own information systems and to attack one's adversary information systems. Thus, the concepts of C^3 and IW are complementary but separate and distinct. C^3 develops and uses tactical information to execute missions; IW protects friendly information while offering tactical advantage by attacking and/or exploiting the enemy's information systems.

FUTURE NAVAL OPERATIONS AND INFORMATION REQUIREMENTS

Chairman of the Joint Chiefs of Staff, General John M. Shalikashvili, USA, in his Joint Vision 2010 of future warfighting,[1] emphasizes four key operational concepts that embody improved intelligence and command and control: (1) dominant maneuver, (2) precision engagement, (3) full-dimensional protection, and (4) focused logistics.

- Dominant maneuver embodies the multidimensional application of information, engagement, and mobility capabilities to position and employ widely dispersed joint air, land, and sea forces to control the battle space and attack critical enemy locations in a sustained and synchronized manner.
- Precision engagement enables naval forces to locate and identify the target quickly and accurately, employ sufficiently lethal weapons to nullify the target, determine the impact of that action through battle damage assessment (BDA), and reengage the target as necessary.
- Full-dimensional protection requires control of the battle space by providing multilayered defenses against all types of enemy threat capabilities.

[1]Shalikashvili, John, GEN, USA. 1996. *Joint Vision 2010*, Joint Chiefs of Staff, Washington, D.C.

- Focused logistics involves the capability to provide rapid materiel response, to track and redirect assets even while they are en route, and to deliver tailored logistics directly at the tactical level of operations.

Naval forces can be expected to employ these concepts in the conduct of naval missions throughout the late 1990s and well into the 2035 time frame in operations ranging from the "violent peace" environment with operations other than war (OOTW) to major regional conflict (MRC) and full-scale war. Many of these missions will focus on the primary task—to deter conflict—and will involve both strategic and tactical forces operating as a deterrent to aggression by hostile forces, to provide a forward presence and project military power on a global basis. In addition to the role of naval forces as a component of the strategic nuclear deterrent, it is expected that the main emphasis will continue to be on littoral warfare environments, where the full range of tactical operations will be conducted, including:

- Precision strike,
- Antisubmarine warfare,
- Mine countermeasures,
- Air defense,
- Amphibious assault, and
- Theater ballistic missile defense.

As indicated above, the success of these missions will couple tightly to the commander's capability to develop and maintain timely, accurate, and complete information on all aspects of the projected battle space (i.e., situation awareness) and to protect it from enemy intrusion and disruption.

The principal components of the commanders' information requirements bracketing the area of responsibility (AOR) will include (1) the multidimensional (land, sea, air, space) order of battle with disposition and location of own, enemy, and friendly forces located in a common geographical coordinate system; (2) intelligence summaries that provide information on enemy intentions and capabilities; (3) data on environmental conditions (oceanographic, bathymetric, terrain, atmospheric, and exoatmospheric); (4) accurate worldwide mapping, charting, and geodesy; (5) readiness of forces; (6) rules of engagement (ROEs); (7) logistical support (spares and consumables); and (8) administrative needs.

THE ROLE OF INFORMATION TECHNOLOGY

Information technology will be central to future naval operations and will provide a number of tactical advantages to naval forces, including:

- A higher tempo of operations,
- Improved precision and rates of fire,

- Increased effectiveness and maneuver of dispersed units,
- Improved situational awareness,
- Improved battle assessment and alternative courses of action, and
- Increased dispersion and mobility of forces.

The advantages accrue from development and application of several key technology areas associated with the collection, processing, display, interpretation, and distribution of significant information. These areas include:

- Automated decision support systems,
- Advanced and interactive displays,
- Object-oriented and advanced software engineering,
- Distributed control and information systems,
- Knowledge-based systems,
- Interactive data collection and management systems,
- Advanced database systems, including geographic information system (GIS) modeling observations,
- Precision navigation,
- Human-computer interaction,
- Modeling and simulation (especially involving the C^2 process as it interacts with various support systems),
- Active and passive multispectral high-resolution sensors,
- Information processing (especially as it applies to large-scale unstructured data sets),
- Multimedia information systems,
- Wireless digital communications,
- Advanced communication concepts (waveforms, coding, data compression) and radio-frequency systems,
- Wide-band networks, and
- Network interoperability.

These technologies will enhance future naval information capabilities. All naval platforms within a battle group or amphibious-ready group, along with attached and supporting sensors and information transfer systems, will be enhanced in capability as a result of advances in these technologies. For example, the submarine will continue to leverage its advantages of stealth and endurance while expanding its role in battle group operations. The addition of high-data-rate communications through emerging advances in submarine antenna technology is a particularly promising approach that would allow the submarine to share data with the battle group and effectively employ its complement of smart weapons.

Computers

Continuing exponential reductions in the size and power consumption of computers will increase their role in naval systems. Computers will be used to process raw sensor data into information, transform and transmit that information where it is needed, support combat simulations and rehearsals, store and recall data on operational objective areas, launch information warfare attacks, and assess battle damage, among many other potential, and yet-to-be imagined applications.

Memory and storage devices will improve at a pace matching the growing need for increased computational speed and throughput. The growth of object-oriented databases and management systems will support timely access to distributed synchronized systems, with interoperable data models.

Human-computer interfaces will change dramatically from today's tactile devices (keyboard, mouse, track ball, and so on) and will enable broader access by human users through speech recognition and speech generation technologies. Interactive displays will respond to hand gestures and eye movements. Operators will view information in three-dimensional high-fidelity space. Intelligent interfaces will provide assistance in analyzing threats and providing alternative courses of action in response. Displays will use standard symbols or icons that have standard interpretations by joint forces.

Computer-enabled capabilities such as modeling and simulation will provide mission rehearsal and course-of-action planning. Realistic simulations using synthetic forces will enable the development of countertactics and superior weaponry. Using hybrid environments for training joint and combined forces will help in the fielding of superior forces while controlling training and manpower costs.

Sensors

Sensing systems grant an advantage over an adversary by providing an up-to-date picture of the battle space. The future use of unmanned aerial vehicles (UAVs), reconnaissance satellites, and remote air-dropped battlefield sensors will provide an all-weather, multisensor view of the battle space. Images with a resolution of 1 meter or better, accessible at a moment's notice, will be available for worldwide distribution. Remote sensors will pick up heat, sound, and motion in the area of operations. These will be immediately and stealthily forwarded for analysis and targeting. Updates of this battlefield picture could come in near-real time to support immediate retargeting and battle damage assessments (BDAs).

Information Networks

Information distribution and control systems in the 2035 time frame will provide a completely transparent and seamless medium for transfer of information to users. Improved connectivity and capacity will facilitate transfer of video,

voice, and data to the mobile or disadvantaged user. The military will use channels embedded in the global information infrastructure built to support commercial and personal uses. Fiber-optic cable-based backbone networks will provide long-haul virtual circuit or datagram services to local networks at permanent camps, bases, stations, and piers. These same networks will also serve satellite ground stations or other remote injection sites. Commercial systems with military special-purpose adjuncts will provide long-haul trunking connection to mobile platforms in all ocean areas around the globe. Surface action groups, amphibious ready groups, and carrier battle groups will coordinate operations by communicating over radio networks using high-frequency (HF), ultrahigh-frequency (UHF) line-of-sight (LOS) packet switched technologies based on asynchronous transfer mode or its derivatives. These backbones along with satellite links will be interconnected with platform-based local area networks (LANs) that support all applications in use on the platform (see Figure 1.1). Sensor systems will also transport raw and processed sensor data over these communications channels.

Links to shore-based networks will be available through RF LOS, geosynchronous satellite, or surrogate satellite links. Personal communications system (PCS) links will be available through terrestrial base stations or low Earth orbit (LEO) satellite systems. Figure 1.2 illustrates the composite commercial and

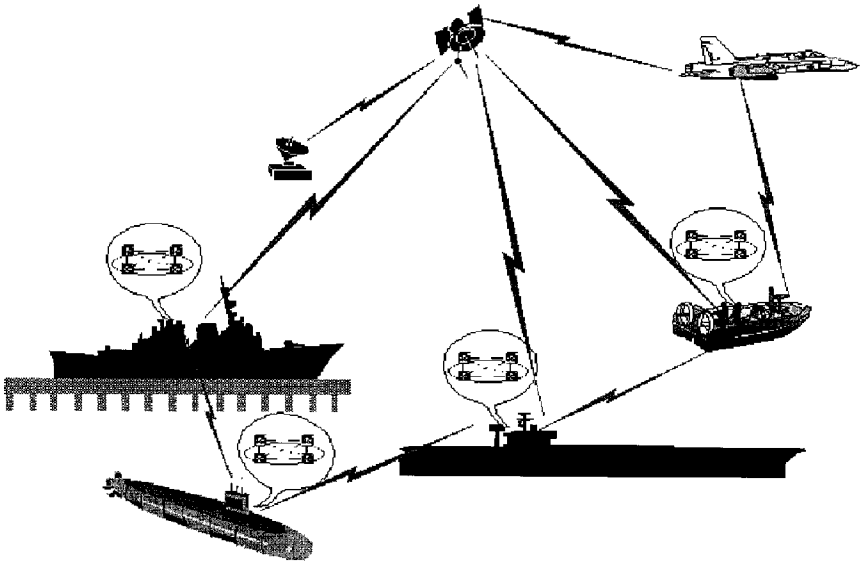

FIGURE 1.1 Networked systems on every platform.

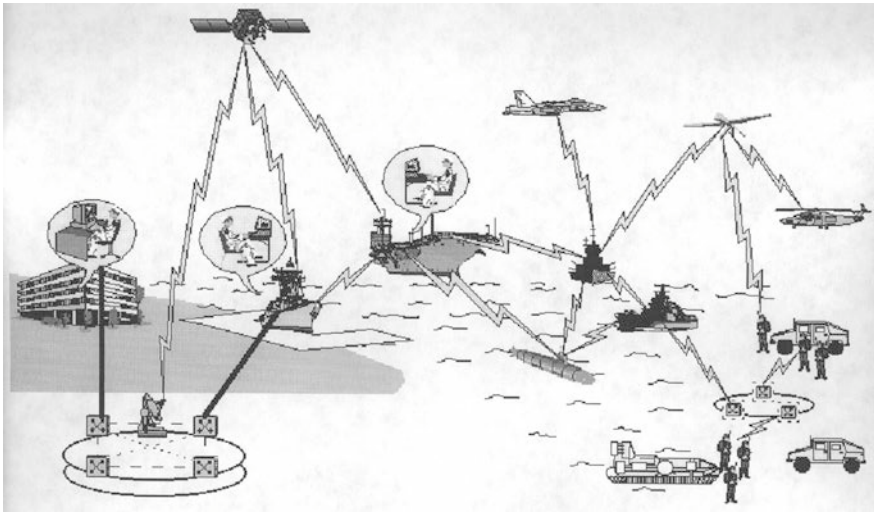

FIGURE 1.2 Ubiquitous wide-band communications.

unique military network architecture and its global extent. The panel envisions that in 2035, problems associated with the availability of connectivity, capacity, and coverage will be largely solved; however, the potential vulnerability of these systems will require special attention. Commercial network infrastructure will provide interconnectivity to the naval forces, and access will be obtained through lease or outsource arrangements.

It is expected that future tactical communications for each platform will have a scaled version of a family of intelligent programmable digital radios. The radios will utilize multiband, multifrequency antennas, coupled to signal conditioning electronics and converters and selectable software to realize a choice of waveform, link protocols, modulation type, and codes. The computing engine will host the software as necessary to perform missions. The associated processor of these radios will also be used for other applications, such as operator training, link testing, and network management and control.

These technologies will help provide a force that has battle-space dominance. Weapons will be delivered precisely from platforms at sea to targets hundreds of miles away with precision and lethality in support of mission objectives. Unmanned sensor systems will be launched and recovered from naval platforms at sea to provide near-real-time multispectral surveillance products fused into a common operational picture. This picture will be used by commanders throughout the joint task force to monitor the tactical situation, redirect forces and sensor systems, and provide battle damage and kill assessments.

Yet such networks and hardware/software capabilities will also expose naval forces to information warfare threats such as denial of confidentiality, data integrity, and service. Techniques must be structured to obviate these threats without a concomitant reduction in quality of service. The networks themselves will need to be engineered to achieve the requisite throughputs and latency requirements needed by the user.

New information systems will be in place to provide worldwide knowledge of weather, as well as a global surveillance and reconnaissance capability. These capabilities will be supported by the ability to correlate data rapidly and automatically from the various sources. The combination of the Global Positioning System (GPS) and a common geo-referencing system will create a synergy among sensor and attack systems. A common data or information model will have been adopted to enable the interoperability of the data that are gathered by the various sensors. There will be a coherent, consistent set of data within the system to provide separate nonredundant tracks on targets of interest. The resolution of multiple tracks on the same object into a single track will be enabled by a world grid referencing system and the ability to provide highly accurate positioning data via the GPS or its derivatives. Through multisensor fusion of tracks and a common information model, databases of tracks will be synchronized and a common operational picture will be available to naval forces worldwide. This capability will be enabled by a communications network that allows access to the data from geographically separate locations on demand. The key to this capability is a common information model, which requires that data be ordered, organized, and parameterized in a structured way to allow consistency and coherence in distributed databases regardless of data sources.

With communications and information handling capabilities in place at distributed geographical locations, it becomes possible for naval force commanders to remotely exercise command and control of their forces. In fact, a better picture of the operation may be available from a remote location because of the robustness achieved through redundant channels or fused complementary data that may not be easily accessed at forward locations if battle damage occurs. Thus the future will provide more flexibility to senior naval force commanders with large support staffs in locating the command support function. This development has broad implications regarding the design and size of platforms to support embarked crew and flag officer staff. Such a concept of operations will be a natural consequence of a robust naval information infrastructure.

The bottom line for the panel's vision of naval communications in 2035 is that any naval activity will be connected to any other naval activity with robust information exchange capability to satisfy all operational needs. This highly networked information capability will be enabled by fiber and satellite communications supplied mostly by the commercial sector, and military-developed wireless tactical networks for platforms operating globally in a wide range of operational postures.

OPERATIONAL CAPABILITIES ENABLED BY INFORMATION TECHNOLOGY

In summary, the emergence of a global information infrastructure providing mobile wireless and fixed services with broadband multimedia connectivity will result in full information utility with unrestricted access and continuous worldwide availability to all friendly forces. The technologies incorporated in this infrastructure will provide naval force capabilities to accomplish the following:

1. Globally manage resources, rehearse missions, provide a common operational picture (i.e. status and disposition of forces, friendly, enemy, and neutrals);
2. Distribute near-real-time tactical and strategic intelligence and sensor information down to the individual unit level;
3. Provide access to intelligence and to environmental and demographic data for mission planning;
4. Provide robust communications connectivity for force coordination, force correlation, and mission synchronization; and
5. Provide ready availability of mission planning and simulation tools to geographically distributed forces.

These capabilities may result in flattened, more effective and more flexible command organizations, better coordination, and improved reaction time. Simply put, information technologies will allow naval forces to fight smarter and dominate the battle space more rapidly than ever before.

ORGANIZATION OF THIS REPORT

In Chapter 2 the panel discusses the evolving global information infrastructure and how the Navy should use it. The panel recommends adopting many commercial components, services, and practices, minimizing Department of Defense (DOD)-unique equipment and standards. With a few exceptions, the panel urges adapting naval use of the infrastructure to what will be commercially available. Because of the special interest of the forward-deployed Navy in satellite communications, the panel also presents, in Appendix B, a history of satellite communications and projects its future.

In Chapter 3 the panel discusses the information content supported by the infrastructure. The panel considers sources, applications, and processing of information content, giving special attention to automatic target recognition (ATR), both by projecting ATR technologies and capabilities and by recognizing the need for the development of a fundamental theory of recognition. The panel also discusses technology for information understanding that transforms data into knowledge, and identifies both likely applications and needs for technology investment by the commercial and military sectors.

Sensor systems are the primary sources of information that is subsequently distributed and understood. Chapter 4 discusses future trends in and technologies for advanced radar and electro-optical sensors. No scientific breakthroughs are needed for improved radar performance, and many improvements will derive from the availability of improved computing elements. A robust commercial airborne and space-based electro-optic sensing capability, described in some detail in Appendix C, is emerging.

With future naval operations becoming critically dependent on information, assurance of the availability, integrity, and confidentiality of that information is vital. In Chapter 5, both the technical and organizational issues involved in achieving assurance and in making information warfare operational are discussed. In Chapter 6, the panel presents its strategy for the Department of the Navy to attain and maintain information superiority over the coming decades, and concludes with 10 specific recommendations.

2

The Information Infrastructure

INTRODUCTION

Success in modern warfare hinges on information superiority not only in surveillance and intelligence, but also in weapons targeting and guidance, navigation, force management, and logistics. The United States, if it must resort to combat to protect its interests, must have armed forces able to achieve and maintain this superiority anywhere in the world, including in the vicinity of an adversary's heartland. In achieving this superiority, the U.S. Navy must reach back to other Services and agencies for information, weld its combat units into a virtual entity of overwhelming power for independent operations, and interoperate with other service components, while relying only on wireless technologies for passing information among its mobile platforms. As the forward-deployed service operating without benefit of forward bases, the Navy particularly relies on remotely provided information support. By necessity, the Navy depends heavily on space systems for communications, navigation, and observation.

WARFIGHTING REQUIREMENTS

The Joint Chiefs of Staff's Vision 2010[1] recognizes the need for a military force to transmit and receive needed information from any point on the globe in a flexible, reconfigurable structure capable of rapidly adapting to changing tacti-

[1] Shalikashvili, John, GEN, USA. 1996. *Joint Vision 2010,* Joint Chiefs of Staff, Washington, D.C.

cal environments. The information infrastructure must support these needs, while allowing force structures of arbitrary composition to be rapidly formed and fielded. Furthermore, the infrastructure must adapt to evolving organizational structures and surging requirements in times of crisis.

The panel believes that the infrastructure must allow information to be distributed to and from anyone at any time: its architecture must not be constrained to support a force-structure (enterprise) hierarchy conceived a priori. Most importantly, the information and services provided to an end user through the infrastructure must be tailored to the user's needs and be relevant to the user's mission, without requiring people at the user's location to sort through volumes of data or images. In the panel's view, the warfighter requires an information infrastructure that:

- Provides robust and reliable service;
- Avoids exposing a user to detection and targeting; and
- Supports force structures of arbitrary composition both by moving information in any format from any source to any destination, and by providing information tailored to the user's needs.

The year 2010 is a reasonable focus for the Joint Staff's *Vision*. The platforms, major national sensors, and weapons available then will be a mix of the platforms available now and those already defined but still in the development/acquisition pipeline. All three take a long time to develop, and, particularly in the case of platforms, stay in inventory for a long time after initial fielding. Because information system technology changes very rapidly, and because information systems can, in principle, be introduced quickly, major changes in warfighting capabilities between now and 2010 will likely depend on new information systems that support the vision.

The period from 2010 to 2035 will likely see the arrival of significant numbers of new sensors and weapons, and the replacement of many naval platforms. It is harder to predict the extent to which new naval platforms will differ radically from those now in service or being developed, but it seems likely that warfighting architectures will continue to evolve in the direction of over-the-horizon fires, information-hungry weapons, and the remote sensors and information systems that they require for their support. Fortunately, the technologies of information systems, particularly satellite communications, on which warfighting architectures must rely, can be expected to advance at an even more rapid pace than the weapon systems themselves (see Appendix B).

Translating operational requirements into information infrastructure characteristics leads to three principles. First, the infrastructure must be based on an integrated, scalable, fully distributed processing and transport environment. It must be dynamically adaptive, self-configuring, robust, secure, and nonexploit-

able. It must be capable of automatically providing tailored information when and where needed.

Second, the processing environment must provide intelligent software agents, hosted on heterogeneous computers fully interconnected by the transport environment, that help get the right information to each user.

Third, the transport requirement must be a network of networks capable of intelligent, adaptive routing of information in any format. The links must be robust and unexploitable, and it is expected that satellite communications will be extensively used for many links.

FULFILLING REQUIREMENTS

Are the components of this recommended infrastructure currently available? Some components that are not yet available for system integration are listed below in the section titled "Technology Investments." Although the discussion above presents the required information infrastructure characteristics in approximate order of descending difficulty, they are examined below in the reverse order, from those that are relatively easy to develop to those that are the most difficult.

Transport Environment

The technological issues concerning the movement of information from one node to another are well understood, and technology is available to meet the warfighter's requirements.

Robust, Unexploitable Links

Because the naval forces are making more and more use of over-the-horizon targeting, cooperative engagements, just-in-time logistics, and so on, they need to be sure that links are available without interruption due to natural causes or enemy actions. They must be unexploitable, that is, immune to platform detection localization, targeting, interception of message content, and insertion of deceptive information.

With the continuing fall in the cost of computer components, it is possible to demand cryptographic security in the transport mechanism and significantly reduce the hazards of exploitation of message content and insertion of deceptive information. Elimination of detection and targeting is possible but more expensive; the available techniques are spectrum spreading and use of directional beams. As a general rule it is not necessary to eliminate completely the signature of a platform's links; it is only necessary to make that signature no easier to exploit than the platform's other signatures.

The cost of spectrum spreading has been the major barrier to its wider use,

but that cost is decreasing due to advances in the manufacture of computer components. The use of spread spectrum in commercial systems is growing. The components used in electronically steered antennas are more specialized, and DOD action may be needed to motivate the commercial sector to produce a stream of the necessary components. The same two techniques—spreading and use of directionality—also confer jam resistance.

Intelligent Adaptive Routing of Information in any Format

Routing sends information from source to destination over available links. Military systems need adaptive routing because traffic demands are highly variable over time and because link availability and capacity vary rapidly due to platform motion and combat damage. The ability to send information from any source to any destination is an essential feature of "plug-and-play" warfare architectures.

We see in the commercial world intelligent, adaptive routing both in computer networks and in telephone networks. We also see that networks can generally carry any information, provided that it is suitably wrapped. It is the panel's view that it should not be too hard to meet the warfighter's need with currently available technology.

Military tactical networks, however, often have fixed routing, and many can carry only precisely formatted messages. The Joint Tactical Information Distribution System (JTIDS) was conceived of over 25 years ago at a time when physically small computers were not capable of dynamic routing and store-and-forward messaging. It was reasonable then to envision it as a time-division-multiplex system with relatively fixed slots, and the JTIDS program cannot be blamed for co-mingling levels of the International Organization for Standardization (ISO) model in an era before that model existed. Today, there is no reason for the Navy not to move aggressively toward adaptive routing. As an interim measure, part of the capacity of the JTIDS network could be reserved for an adaptive router of Internet protocol (IP)-like packets. The cooperative engagement capability (CEC) defense dissemination system (DDS), a robust closed system with adaptive routing within the system, cannot carry arbitrary packets to an arbitrary destination within a participating platform. Again, some capacity should be reserved for an IP-like router.

For those nodes that are multiply connected, adaptive routing provides robustness beyond that provided by the individual links.

Network of Networks

Interconnection of networks, each capable of carrying information in any form to any destination within the network, supports force structures of arbitrary

composition. Heterogeneous networks rely on multiple-hop satellite links and fiber-optic cables, as well as open architecture using commercial protocols and standards.

Internetworking is so commonly practiced in the commercial world that we sometimes forget that the Navy does not fully Internetwork in its tactical infrastructure. A specialized converter translates between Link 11 and Link 16 formats, but there is no way to address an arbitrary packet from outside the network to a member. If the intelligent adaptive routers recommended in the previous subsection were implemented, Internetworking would be facilitated.

Information Services

The transport network connects nodes that together perform the services needed to fulfill the warfighter's requirement for information tailored to users' needs. The panel's description of the processing environment identifies four important characteristics of the environment.

Hosted on Distributed Heterogeneous Computers

Unless the required information services can be provided by distributed networks of heterogeneous computers, the Navy will have to continue requiring uniform "standard" computers, a policy that condemns the Navy to lag the state of the art, makes upgrades appear unaffordable, and fails to recognize platform-specific requirements.

The Internet would not have grown if every participant had to own a "standard" computer or even a "standard" operating system. The Navy should learn from this model. Clearly, the requisite technology is commercially available.

Provided by Intelligent Software Agents

In the "Warfighting Requirements" section above, the panel cited the warfighter's need for an information infrastructure that provided information tailored to users' needs. The panel believes that this will be one of the major challenges of the coming decades. Great progress was made in the 1980s in making high-performance computing available in small, affordable packages, and the panel expects this progress to continue. The 1990s saw an explosion of Internetworking with great progress in integration, interoperability, and collaboration through the use of open architectures, protocols, and standards. The Army seems committed to these architectures. However, these technologies can cause an information glut. We will need the capability to assemble voluminous information in a reasonable way for a particular user and to make inferences from the assembled set.

Meeting the warfighter's need for tailoring of information can be accom-

plished through the use of intelligent software agents[2] (ISAs) that are aware of a user's situation and needs, will gather the information that will fulfill these needs, and will provide the information in a convenient form, all without requiring a specific request from the user. Because of the distributed nature of the architecture, these agents can reside at multiple locations, optimized for platform and transport considerations.

For example, if there are many users with different needs located on large platforms, then it may be convenient to have a single broadcast with agents at each user's location plucking the information relevant to that user from the broadcast. Conversely, if the users are dismounted Marines, the agent for each user might reside on a computer located on a large platform—a communications channel would be dedicated to the user, and the user would need to carry only a radio and a rich human-computer interface.

Intelligent software agents can also perform format translation, providing an alternative to the present system wherein message formats are rigidly standardized, standards are modified at a glacial pace, and each change in standard engenders expensive software redevelopment. Because they are migratory, a node that does not have the capability to "understand" a message can acquire the capability over the infrastructure.

The need for intelligent software agents to perform data mining exists in the commercial as well as in the military sphere. Although there may be considerably synergy in inference engines and system-building tools, it is not clear that commercial products will meet naval needs.

Integrated and Scalable

Integration and scalability fulfill the warfighter's requirement to support force structures of arbitrary composition.

Capable of Automatically Providing Tailored Information When and Where Needed

This capability can be provided by the combination of intelligent software agents distributed among nodes and the transport environment that interconnects the nodes. However, integration implies that the agent understands more than the local situation and can adapt its behavior to changing needs.

---

[2] A software agent provides a service or function on behalf of its owner; an intelligent software agent is likely to be autonomous, goal directed, migratory, and able to create other entities. An example of a software agent is a filter that processes mail, or a newswire, and presents to its owner only that information likely to be of interest. Whether an agent would be considered intelligent is likely to hinge on the degree of specificity with which it must be instructed.

Dynamic, Adaptive, Self-configuring, Robust, Secure, and Nonexploitable

Dynamic, adaptive, and self-configuring systems are enabled by the adaptive routers. Information infrastructure is robust for two reasons: (1) links are made as robust as is economically feasible, and (2) most nodes are multiply connected, with the adaptive network automatically reconfiguring to take advantage of uninterrupted links.

Security and nonexploitability result both from the use of waveforms that resist jamming, others that enable identification and geolocation, and where appropriate, from the use of directionality that resists both. Adaptive routing can ameliorate some of the difficulties arising in systems with directional links. Security and nonexploitability also are enhanced by cryptography, which prevents unwanted extraction of information from, and insertion of false information into, the information infrastructure.

However, the integrity of information must be protected from flaws and corrupt information accidentally or deliberately introduced into the infrastructure before it was fully constituted. Intelligent software agents could possibly help detect these possible sources of damage, isolate them, and reconfigure the infrastructure, but the technology does not exist today.

IMPLEMENTATION

Implementation of the envisioned tactical information infrastructure will require policy actions, system acquisitions, and technology investments.

Policy Actions

Needed policy actions include the following:

- Commitment to information superiority through adequate provision of resources, timely incorporation of innovation, strong defense of our information and information systems, and preparations to degrade an adversary's information and information systems;
- Adoption of commercial standards and equipment, and adaptation of naval practices accordingly;
- Standardization at the proper level, e.g., routing wrappers, and the use of software radios and ISAs to permit introduction of new waveforms, formats, and services; and
- Exploitation of the organizational flexibility arising from a powerful information infrastructure.

Committing to Information Superiority

The United States military now enjoys a substantial information advantage over potential opponents. Information dominance was a key factor in attaining victory in the Kuwait theater of operations while sustaining very low casualties. We must be careful not to let this crucial advantage slip away.

As force levels shrink and as precision weapons permit victory with smaller forces, the fraction of the defense budget devoted to information would be expected to increase. The panel observes, however, that the ratio has remained fixed. A mechanism is needed to rebalance investments in information, platforms, and weapons in terms of the new warfighting architectures. Lacking such a mechanism, the likely outcome will be that next year's budget share will be based on the past year's and that sunset and sunrise systems will be drawn down together.

We could lose our advantage through complacent acceptance of the traditional delays in introducing military innovations. Major military systems often require 25 years from conception to full deployment; computer systems become obsolete in a tenth of that time. An agile opponent could deploy systems with state-of-the-art commercial technology while we were using systems of much lower performance.

As the military adopts open architectures, it will become technically easier to upgrade systems, but procurement habits change slowly. These upgrades can be accomplished through advanced concept technology demonstrations (ACTDs) with a very abbreviated development and evaluation cycle. Secretary Perry recently noted that "full implementation of legislative and regulatory changes enacted two years ago will allow the department to save literally billions of dollars as well as to rapidly incorporate cutting-edge technology into the military's weapons systems."[3]

Because information systems are key to U.S. warfighting capabilities, we must defend them against enemies seeking to deprive us of our advantage. The panel pointed out above the requirement that information systems be robust, but there are other actions that need to be taken, including training information system operators to be alert to the possibility of attack and to know how to reconfigure networks and to continually probe our own systems for vulnerabilities.

Conversely, we should be prepared to degrade an adversary's information systems through conventional, electronic, and cyberspace warfare.

The maintenance of information superiority in face of the threat of enemy information operations will require skilled and motivated people. However, the panel is aware that when the Defense Intelligence Service Agency (DISA) and Fleet Information Warfare Center (FIWC) attempt to penetrate military computer

[3] Perry, William J. 1996. "Defense in an Age of Hope," *Foreign Affairs*, 75(6): 64-79.

networks, they usually succeed and are seldom detected, even when they use simple, well-known, penetration methods. The Navy is introducing courses to increase the skill level of information system operators, administrators, and security officers, but the success of this approach hinges on the availability of high-quality people in both enlisted and officer pipelines.

Unfortunately, even though warfare is becoming more information-centered, the people who make it possible are still at a disadvantage in competing for promotion with people in traditional warfare specialties. When RADM Bell, a submariner, became Director of Naval Communications, he considered it a career negative, stating, "The volume entitled 'Famous Naval Communicators' is very slim." Unless naval personnel well skilled in the information technologies are treated with respect and have clear paths for career advancement, they will defect to the civilian sector where their skills are in high demand.

Adopting and Adapting

Commercial interests will continue to drive the development of most information technologies, and the Navy must be prepared to accommodate rapid changes in the direction that commercial capabilities evolve by adopting commercial technologies and equipment and adapting naval practices and systems to incorporate them.

Although many developers of military information system claim that they are using COTS products, closer inspection often reveals that they have adapted the commercial product. Adaptation is markedly less desirable than adoption because in upgrading products commercial suppliers protect customers who have adopted previous generations, while a naval customer who has frozen on an earlier version and adapted it to his needs will lose the benefit of product upgrades and may end up with the burden of maintaining the system. Instead of adapting COTS systems to naval practices, the Navy should lean toward adopting commercial products and adapting the naval processes that use them.

Standardizing Selectively

The folly of attempting service-wide standardization on a single model of a computer is now well understood, but there are some things that need to be standardized within the tactical infrastructure. The panel believes that a standard way of indicating information sources and destinations is needed, although ISAs at various locations could deduce additional destinations toward them. Obviously waveforms at both ends of a link need to be identical, but that waveform can be adapted to conditions through software radios.

Agreement on the meaning of transmitted data is clearly required, but alternatives to the present practice of promulgating standard software suites that are changed infrequently should be investigated. Precedents exist in commercial

practice: a node can acquire over the network "applets" to perform a service not native to that node. A tactical information infrastructure with ISAs should be able to accommodate new formats and services almost as easily.

Ensuring Organizational Flexibility

Supporting force structures of arbitrary composition will require considerable coordination at the execution level even though some of the command structures of executing units may be absent. Implementers of the infrastructure should avoid the error of enshrining the current military organization chart in the architecture. Experience in the business world demonstrates that rich information infrastructures lead to changes in the organization chart. While the armed forces will reorganize at their own pace, the infrastructure must not be an impediment to reorganization.

System Acquisitions

Four of the elements of the tactical information infrastructure—adaptive routers, robust links, relay proliferation, and open systems—are sufficiently mature for acquisition, given adequate budgets and policies.

Adaptive Routers

Although control algorithms better than those currently available may be desired, it is not too early to plan the acquisition of adaptive routers and choose a wrapper format. Adoption of other than a commercially successful format would require very compelling reasons. Much can be done now in acquiring components of the transport environment.

Robust Links

The three major options for robust military-only links are, in descending order of capacity and robustness, extremely high frequency (EHF) as it will evolve in MILSTAR II and successors, Link 16, and very high frequency (VHF)/UHF software radios. The CEC DDS is also a robust, high-capacity system, but the panel doubts that it will proliferate outside the Navy. Lightweight, deployable EHF terminals have been developed and should be acquired as soon as compatibility with future processing relay satellites is assured. The Navy is committed to Link 16, although the $1 million price of the JTIDS terminal and the $500,000 price of its multifunction information distribution system (MIDS) successor is slowing deployment. It would deserve wider deployment if it could be made a more open system, if terminal prices could be reduced, and if its frequency spectrum could be protected from the Federal Aviation Administration (FAA)-

imposed restrictions. The software radios offer robust low-data-rate communication. Although they probably will be initially programmed to the single-channel ground-to-air radio system (SINCGARS) waveform for backwards compatibility, their programmability can be exploited in adaptive architectures. Open systems architectures enable the same encryption technology to be used in many applications and thereby increase production volume and lower prices.

Relay Proliferation

System robustness derives not only from robust links but also from a proliferation of links. In addition to the military-only relay satellites, commercial relay satellites, including new low-altitude systems, will provide additional links. The two leading acquisition issues are terminals and antennas for multiple links and whether additional military-only relay platforms should be acquired.

Tri-band terminals have been developed that can operate in either the commercial C and Ku satellite communication bands or the military X band. Ships, in particular, need multibeam antennas capable of maintaining several such links simultaneously, as well as several dedicated common data link (CDL) sensor links.

UAVs offer additional military-only relay capacity. The panel urges that any new military relay platform be equipped with routers functionally equivalent to those found at system nodes, rather than predesignating the services that each class of relay platform would offer.

Open Systems

Actions should be taken now to put ports on such closed systems as JTIDS on CEC DDS for router access throughout the infrastructure. The concept of separating the message content from the means of transmission implicit in the variable message format (VMF) that the Army applies to its use of software radios should be embraced by the Navy.

Technology Investments

Although some information infrastructure elements are ready for acquisition, technology challenges remain in providing the following:

- Components for robust links;
- Means to adopt appropriate commercial information technology without assuming poorly understood risks;
- Architectural integration of heterogeneous systems, including adaptive, flexible human-computer interfaces and appropriate network-of-network protocols;

- Adaptive transport protocols, including incorporation of appropriate commercial Internetwork protocols; and
- Means to develop intelligent software agents, including those for knowledge representation and intelligent action.

The panel believes that the two areas particularly requiring near-future DOD technology investment are the information assurance aspects of risk management, ISAs, and system integration.

Components for Robust Links

To meet the need identified above for adaptive multibeam antennas suitable for naval platforms, a number of technology-base programs have been proposed, but none has been adequately funded.

Links, whether wireless or cable, require cryptographic devices to prevent exploitation and deception. Commercial interest in electronic commerce has motivated the development of commercial cryptography with good products that will likely improve. Policy, however, gives the National Security Agency (NSA) total authority over the encryption of national security information.

The heart of a cryptographic system is its key generator. The NSA has developed a low-cost, computer-compatible card (Fortezza) incorporating approved key-generation algorithms. However, the Fortezza card itself must be imbedded in security services software, which has not been developed. If the Fortezza card were to incorporate the interfaces of the commercial software cryptography systems, the DOD would be relieved of the burden of maintaining and improving security services software but would still maintain control of key generation and distribution.

Means for Adoption of Commercial Technologies Without Assuming Poorly Understood Risks

Warfighting systems require a high degree of assurance, higher than that provided by most commercial systems. In our desire to exploit commercial technology, we must not introduce security hazards. The panel identified six candidates for DOD investment; none of them is Navy-unique.

Four candidates can be classified as information service elements:

- Detection of flaws, corruption of information, and information warfare attacks;
- Building of assured systems from insecure components;
- Automatic fault detection, reconfiguration, and load balancing; and
- Dynamic security policy dissemination, arbitration, and enforcement.

These candidates, and particularly the second, which concerns composition, reflect the fact that commercial products may not be individually strong, and that the panel's recommended policy of adopting products and adapting the way naval forces use them requires fixing this deficiency at the system level, rather than trying to modify the commercial products.

Two candidates pertaining to the transport infrastructure arise from the desire to push the open systems architecture as far as possible for use in combat. Although breaking the barriers between stovepipes reduces average delays, it is necessary to understand how to respect deadlines on time-critical functions. Therefore, the panel recommends investment in the following:

- Dynamic resource management, and
- Meeting deadlines.

The inevitable inclusion of commercial links and services in the DOD's information architecture requires assurance of their availability in times of stress. Both technical approaches (e.g., dynamic routing) and policy action (e.g., becoming an anchor tenant on commercial systems) will likely be needed.

Network Integration

A vibrant commercial network integration industry already exists, but some effort will be needed to integrate legacy military networks. Establishing gateways is an obvious solution, but better methods should be sought.

Adaptive Transport Protocols

The panel's instinct is that the DOD should follow the commercial mainstream protocols, but it recognizes the need to investigate their suitability for naval force needs. For example, most dynamic routing protocols assume that while information traffic may vary considerably, the switching nodes move seldom or never and that link failures are uncorrelated with each other and with node outages.

Intelligent Software Agents

Intelligent service application software agents must provide tailored, human-centered data acquisition and processing, data fusion, and information generation and dissemination to users. These agents act to deliver processed, synoptic information rather than volumes of data and images. A function such agents serve is rapid search and discovery of geographic knowledge. The basis for such search is often geographic location. The object is to retrieve all data and information concerning a place. These data and information must be retrieved and

organized into a form from which the user can effectively and efficiently extract required information. The service application software agents collaborate with other software agents to achieve general goals set by users, and based on user profiling, generate pertinent situation changes that may be of interest to the user. The agents support automatic, dynamic, adaptive allocation of transport and processing resources, and replicate as necessary for efficiency and to ensure continuity of services provided to the user.

Intelligent application software agents must provide an array of functions appropriate to the user's mission and situation, and exchange information and status with other application software agents to provide integrated yet distributed execution of requested user services. These agents automatically select and perform their functions depending on specific user requirements and profiled user interest areas. The agents provide discovery and integration of text, tabular and geospatial data from multiple, heterogeneous databases, broker between other agents for sharing of information, and negotiate with service agents to establish appropriate network and resource allocations to achieve their goals. These agents are adaptive, in that they profile user needs for information such as measurements, targets, maps, changes in areas, and models against direct user input, past user requirements, and an understanding of user mission, status, and intentions.

Although successful examples of both types of agent exist, there is general agreement that more investment to strengthen the technology base is needed before robust agents can be routinely constructed. This is not trivial. As the nation attempts to integrate DOD and commercial geospatial data, many important questions remain open. Needed technologies include:

- Universal language and computational models for declaring agents,
- Representation technology for knowledge and system resources,
- Algorithms and protocols for agent management and interagent negotiation and information exchange, and
- Automated learning and user-profiling techniques.

Because of commercial interest, DOD need not pay the entire bill, but the pattern in the past has been one of DOD investment in high-risk developments and commercial investment in turning the successful developments into products. Even if this pattern is broken, some DOD investment is needed in domain-specific developments.

3

Information Content

INTRODUCTION

The previous chapter discussed the information infrastructure to support information superiority. This chapter examines issues related to the content that will be carried by that infrastructure. In particular, this chapter focuses on three aspects of information that affect the value and utility of information content: (1) sources, (2) applications, and (3) processing. Sources of information are proliferating, and many new publicly accessible sources will be utilized by the naval forces of the future. Applications that manipulate information content are highly varied but can be classified according to requirements for timeliness of the application outputs. Certain applications require rapid decisionmaking based on deliberately acquired information, whereas other applications will use intelligent software agents and other means to probe large preexisting databases. Finally, improved processing methods enable applications to be executed more efficiently, thus enhancing the value of information content. Automatic target recognition (ATR) requires advanced algorithmic techniques and is an example of a class of applications where current limitations on processing capability represent a significant impediment to implementation. ATR can be viewed as a special case of information understanding that uses algorithms to recognize patterns in databases of information.

From the user's point of view, representation is an essential aspect of information content. How information is presented, whether to a human operator or to an automatic analysis system, is often a principal determinant of its utility. Information can also take on new significance when organized in useful ways. The

Department of the Navy has a particular need for compact representations of information because of the constraints imposed by the relatively limited bandwidth available for ship-to-ship and ship-to-shore communications.

Information content conveyed to the warfighter at any level of command is the end product of a system that is integral to the security of the nation. The information system, consisting of the infrastructure, information content, sensors, and security systems to safeguard the information, forms an essential asset in the repertoire of defensive systems, on a par with platforms and weapons.

INFORMATION SOURCES

The continuing development of inexpensive, powerful processing capabilities ensures that the coming decades will be marked by ongoing advances in information technology. Increasing access to advanced information processing and information management capabilities will lead to a proliferation of activities that generate, maintain, manage, and exploit information, and it is certain that the military will be one of the many important players in the new world of information-centered activities.

The DOD and the Department of the Navy need to be in a position to exploit a wide variety of available information sources. Certain of the military's information needs are unique and highly specialized, and will require focused investment to develop the requisite technology. This is particularly true in the area of mapping, charting, and geodesy. Here, continued R&D and infrastructure upgrades will be required to produce geospatial data for the warfighter in a timely fashion. Other needs, which may be less unique and less specialized, will be met by appropriately exploiting sources of information that will be available in the public domain.

New sensor systems and the increasing use of indigenous sensors are emerging from the dramatic growth of the commercial communications infrastructure, and the data they generate represent a new class of public-domain information. These systems can be classified into two categories: commercial systems that will be developed in order to sell information for profit, and sensors used in conjunction with information systems for the benefit of the user. The first category includes commercial satellite imagery, databases and mailing lists available for purchase, and commercially operated data mining sources. The second category includes automobile sensors communicating with a "smart" highway; smart homes providing communication links between appliances and manufacturers for maintenance and monitoring; remote camera systems operated by organizations for the benefit of the public, such as town-square imaging systems accessible over the World Wide Web; and water measurement sensors that transmit reservoir fill levels to public water works. Together, these two categories constitute an enormous body of information that, typically, will reside within the public domain, and from which it may be possible to extract, for example, data

regarding the location of an individual or vehicle, or the state of a particular system at any given time. This type of information will become increasingly available to friend and foe alike. The Navy and Marine Corps can either attempt to exploit the information in a way that is more timely and deeper than all potential adversaries, or can attempt to deny the information (or utility of the information) to adversaries. While a balanced approach is advisable, it would be prudent to assume that all information is persistently available to all parties, and that information superiority will be derived from greater awareness, planning, and exploitation capabilities.

Accordingly, it is incumbent on the Department of the Navy to position itself such that it is capable of exploiting this rich new class of sensors and information. In some cases, directly relevant information can be purchased or procured. More often, however, the required information must be inferred from public sources and those inferences then transformed into a form relevant to Navy Department needs. For example, publicly accessible town hall sensors and reservoir data can be used to infer local conditions. Traffic analysis can indicate levels of activity, and movements of individuals can indicate deployments. Information on local conditions that can be inferred from the direct data could be extremely useful when appropriately presented to a commander or operator. Data mining technologies and collaborative filtering techniques can be used to deduce information and compact it succinctly for analysis and presentation.

Indeed, the body of information that will be available can, if properly exploited, lead to a revolution in the intelligence field, and provide the data sources for intelligent software agents and automated inferencing engines that can be crucial to Navy and Marine Corps missions.

APPLICATIONS

The utility of information depends, in large measure, on applications that take raw data as an input, analyze them, and transform them into a representation that is meaningful to operators and commanders. This task is so demanding that, ultimately, a new class of applications technology will be required, which could be called information understanding, and which will include a suite of advanced methods for processing, analyzing, and representing information. Information understanding could greatly extend the capability of ATR systems, for example, as well as other technical means of gathering intelligence. Such enhanced capability could be important not only for target recognition using sensors designed to acquire battlefield information, but also for reasoning about disparate information sources on a longer time scale, to provide deep understanding and facilitate planning for potential military operations. Traditionally, sensor information is fed to a processor that performs pattern recognition functions in order to detect targets. This methodology assumes, however, that sensor data is a rare and precious commodity that must be processed immediately. It also assumes that the

relevant information is localized in a sensor stream. In a sensor-rich environment, the timing of the processing can be matched to the requirements of the application. New applications for the exploitation of sensor information are afforded by the ability to consider processing outputs from multiple disparate sensor sources over longer periods of time.

As mentioned above, certain applications require that decisions must be made immediately, and so require rapid access to information with minimal latencies. Other applications make decisions that are based on information that has a long time constant, and thus might involve processing times that could involve hours or days or weeks. As such, these applications can afford the luxury of accessing massive databases. If the processing must occur in time t, and the bandwidth is B, then the maximum amount of information available to the application in order to make a decision will be at most tB. In order to make an intelligent decision, a certain amount of information is always necessary, and thus bandwidth requirements are necessarily high for applications that require timely decisions. However, applications that can be executed at a more leisurely pace have the opportunity to make more intelligent decisions by massively increasing the total amount of information available to the processor, either by virtue of the additional time, or through large bandwidth capabilities, or both. Accordingly, requirements for timely decisions impose constraints on the amount of data that can be accessed, whereas longer-term applications can access large, distributed, disparate databases and make use of more intensive intelligent processing. This relationship is illustrated schematically in Figure 3.1.

Not only is there a tradeoff between timeliness and the amount of information accessible to the process, but the kinds of information sources that are useful will also be affected by the type of application. The value of some information decays over time, and applications with long processing times will, in general, only be utilized for processing information whose value persists over a reasonable time scale. On the other hand, applications that make relatively fast decisions will need immediate access to timely information, and thus will likely be tightly coupled to sensor systems.

Indeed, there is an overriding need for awareness of what information is available and where it can be located, as well as for timeliness and assurance of the information sources. With such awareness, information can be matched to the application, and action can be taken in advance to ensure that the information will be available when needed. Finally, it is important to be able to perform inferencing, to adapt information to representations that are useful for military needs, and to fuse information from multiple sources. Naval forces have a particular need for automated inferencing for many applications due to the comparatively limited bandwidth that will connect naval platforms to the information sources. That is, while shore-based human analysts will be able to make deductions based on presentation and visualization of massive databases connected by ever-increasing fiber channels, analysts resident on naval platforms will have to

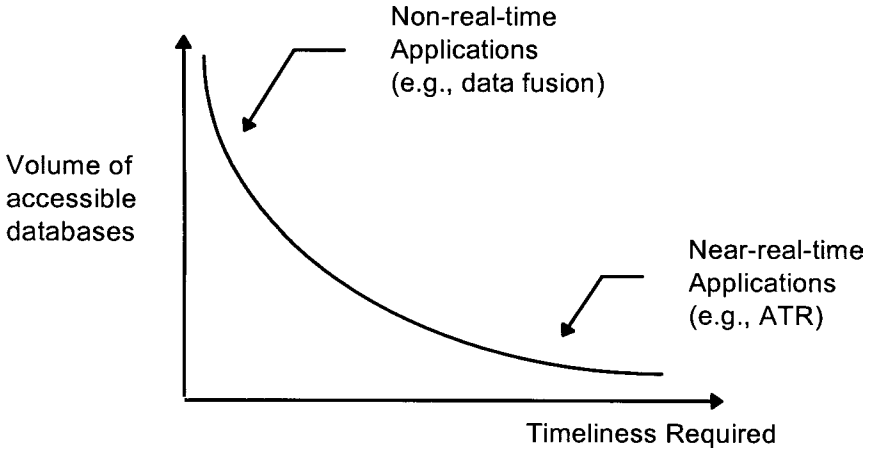

FIGURE 3.1 Categorization of information applications.

work with data streams that are constrained by satellite and radio connectivity. Processing that performs inferencing and transformation of information is thus required not only to aid the interpretation, but also for compression.

Considering the proliferation of information sources, and the need to match sources to the classes of applications, it is incumbent on the defense establishment to develop an awareness of the available information. In order to perform these functions and to ensure timely and convenient access to those sources by naval assets, responsibility should be designated within the Department of the Navy for the identification, organization, and classification of all relevant information sources. Assembling links to information sources will include awareness of novel information providers, creation of maritime-specific databases, mirroring of certain databases for rapid accessibility, and vigilance in the maintenance of the quality of the databases.

PROCESSING OF INFORMATION

The growth of the information infrastructure and the proliferation of new information sources will enable new ways of exploiting information for military purposes. As discussed above, some applications require rapid decisions and are thus tightly coupled to local sensor streams, whereas other applications can make use of massive databases and can perform automated intelligence operations through processing occupying longer periods of time. More advanced algorithmic methods will be required to facilitate extraction of useful content from massive information databases. For example, there is a clear need for more effective means of using sensor data to locate targets, which is a special case of the recognition capabilities that typify the military uses of information processing.

The civilian financial sector has a similar need for advanced recognition capabilities, and commercial interests are currently helping to drive the development of database mining and information fusion techniques. Because of the critical importance of information to military systems, however, the Defense Department should strive to remain in the forefront of ongoing developments in this area Yet, before recognition capabilities can be developed that extend target recognition in localized sensor data, generalized capabilities for automatic target recognition need to be successfully demonstrated and refined.

The Department of the Navy should develop capabilities in information understanding by identifying database mining methods that are applicable to defense needs, and by funding research in the broad area of recognition theory. However, as a base, ATR technology should be assessed and understood in a broad context by the Navy and the Marine Corps. A summary assessment is presented below, together with some hints at a unifying theory. The intention of the following discussion is to develop a basis for the more general discussion of information understanding that makes up the balance of this chapter.

AUTOMATIC TARGET RECOGNITION

Introduction

With naval forces continuing to take the leading role in power projection and management of the early stages of regional conflicts, a central focus of technology for naval forces will be the determination and tracking of targets. The environment is necessarily target-rich and will likely pose difficult problems for target recognition algorithms, with targets and nontargets in close proximity. The ability to distinguish between targets and non-targets automatically and non-cooperatively is generally considered to be the province of automatic target recognition (ATR). Despite the fact that ATR technology is not yet mature, it is already clear that this technology will be an essential component of naval activity in the future. The Navy has a particularly high stake in the ability of ATR to effectively distinguish among target types, in order to provide accurate on-site intelligence in advance of conflicts and to properly, efficiently, and safely effect strike missions during conflicts.

One cannot expect a single black-box that will work for all scenarios and all applications and, in general, ATR is not a single technology per se, but rather a suite of technologies that incorporates a variety of approaches tailored to varied target acquisition scenarios. Indeed, the variety of ATR algorithmic approaches will likely continue to mature for several decades to come, and the ability to rapidly train a system on new target types, and to adjust to new environments, including concealment and introduction of decoys, will remain challenges. On the other hand, there already exists ATR technology that shows military significance for automatic cueing of potential targets.

Classification of ATR

Automatic target recognition refers to the ability to recognize instances from a collection of models given sensor data and other information, and to be able to effect recognition despite viewpoint variations, occlusion, obscuration, camouflage, deception, model variability, and other confounding factors. The panel identified the following three application domains for ATR:

- *Surveillance*. The goal is to locate and track targets from a distance, and the emphasis is on detection; there is typically a less urgent need for identification. Often, surveillance involves cueing a human operator.
- *Battlefield awareness*. The emphasis is on identification, particularly of friend, foe, or neutral, and integration of multiple sensor modalities and multiple data sources is highly desirable.
- *Precision guidance*. The emphasis is on accurate orientation and pose estimation in order to perform course correction and other functions related to positioning.

Note that these application domains are distinguished by a timeliness requirement, although even in the case of surveillance, ATR typically connotes a relatively short time scale, involving perhaps a maximum of a few hours. In the case of precision guidance, decisions must be made on the millisecond scale.

Naval forces in the future will make use of advanced technology in all three areas to support missions. Despite slow progress in fielding working ATR systems, it is likely that both continued progress and technology breakthroughs will lead to performance capabilities in all these areas that exceed human recognition capabilities and that can be executed at speeds that would have been unimaginable to image analysts a few decades ago. Progress in processors, memory, and sensors, as well as improved algorithmic techniques for processing signal data, image formation, and coherent combination of information (such as from moving targets), all point to major advances in a very few years.

Sensors and Automatic Target Recognition Everywhere

Automatic target recognition can be thought of as a bandwidth enhancer. Given the need to transmit information about targets and threats to the commanders in as succinct and timely a manner as possible, ATR allows the naval forces to concentrate on the information that is explicitly required, dropping (preferably early in the transmission chain) what is irrelevant or redundant, such as distracting background and clutter.

Once transmission requirements are reduced, then the ATR products can be shipped everywhere, and knowledge of the battlefield, and indeed targets in the world, can be made accessible on demand everywhere. In much the same way

that Internet capacity is providing wide access to information, increasing transmission capacity, provided by the global information infrastructure, will provide increased information access to warfighters. The panel envisions a world replete with sensors, in UAVs and satellites, the potential battlefield area, third-party sources, traffic lights, and even people's hats. These data will be widely accessible, but, in their totality, overwhelming.

ATR systems will likely be placed as close to the sensors as possible in order to minimize bandwidth needs, although in some cases sensor data will need to be acquired through a network, perhaps at great distances from the actual sensor. Ultimately, there will be a long list of target types that can be located and tracked from any position in the world.

One could imagine an Internet-like system where, given the appropriate permissions, a user could call up a view from any location of any other location, in order to be cued to targets and threats of interest. When the synthetic view corresponds to the viewer's current position, then the system gives the capability of looking around corners, through walls, and over hills and mountains.

Technology to Achieve This Vision

Considerable technological advances are required before the vision outlined above can be realized. Military needs are in some cases special and will require focused development. Some of the required advances are formidable, but others are straightforward, given sufficient attention and resources. The panel anticipates that these advances can occur in many different nations but are most likely to occur first in the United States, providing that sufficient attention is focused on ATR development.

Synthetic aperture radar (SAR) is currently the principal means for acquiring sensor data for target recognition. SAR's advantages include all-weather capability, high resolution, and imaging at a distance. Infrared sensing, on the other hand, demands proximity, but can provide extremely useful information at high resolution by passive means. It must be assumed that the suite of available sensor modalities will expand, and that ATR methods will be able to provide generic, multisensor recognition capabilities.

Technology advances are anticipated in the following three areas:

- Better sensing methods,
- Better algorithmic methods for performing recognition, and
- Faster and better computer processing.

In the area of improved sensing, SAR image formation methods can be considerably improved. New methods for improving the resolution, for coherently adjusting and improving the combination of raw signal data, and for adap-

tively forming the best image promise to dramatically improve SAR capabilities for ATR applications. While the capability does not exist today, it may be possible in the future to form SAR images of moving objects. Some progress has been made in this area, but the algorithms are more delicate. It is reasonable to expect that developments will occur to permit high-accuracy radar imaging of moving objects at long distances. Much of the Navy Department's investment in ATR development has focused on the inverse SAR (ISAR) modality, such as imaging a moving ship from a fixed radar platform. These algorithmic methods for image formation, applied to other targets such as moving ground targets, may prove useful for achieving high-resolution imaging of moving targets at a distance, although at this point, the use of ISAR techniques for general ATR applications is only in the earliest stages of development.

Inexpensive infrared (IR) sensors, especially ultraminiaturized sensors, are likely to be available in the near future. Depth sensing, by light detection and ranging (LIDAR), and chemical analyses from a distance might also enable a wealth of discrimination capabilities. ATR is normally associated with image processing, but other signal data such as hyperspectral and multispectral techniques can be used as well, as long as the information assists in discriminating among targets and non-targets. Since the image formation process can involve discarding information, there may be improved methods that deal directly with raw sensor data.

Better algorithmic methods are also likely, but there is a pressing need for a theory that provides a basis for comparing ATR approaches. The components of such a foundational theory are sketched in the next section. Currently, algorithm development in the ATR field is mostly a matter of art and parameter tuning, and the resulting software codifies methods as opposed to real algorithms. The academic fields of computer science and information systems are still organizing into subdisciplines, and computer science is rapidly bifurcating into theory and systems areas. Within the systems area, experimental computer science is slowly emerging as that area that concentrates on the development of computer applications. The broad nature of ATR development requires that a certain amount of theory guide the experiments and construction of systems. At this time, there is insufficient guidance in algorithm development, and an insufficient appreciation of the desirability of foundations.

Finally, improved computer processing will aid ATR development. It is a truism that computer processor power is increasing geometrically. More important to ATR development is the increasing capacity for dense memory storage, and high-bandwidth data transfer within a processor. Since ATR involves comparing relatively small amounts of sensor data with large databases of model data, the ability to index into that model data and to rapidly access the relevant objects largely dominates the processing time. Although researchers have long considered simulations that operate in minutes or hours to be acceptable approximations

of potential real-time methods (when specialized processors are applied, or when computer processor power catches up, in order to provide several orders of magnitude in improvement), the inability to test and process large databases of training data has hampered evaluation and subsequent development. Throughput is improving, however, and current workstations are able to run ATR algorithms intended for real-time implementation on large images in under an hour. These speeds provide some capability for large-scale test and evaluation, and several more doublings in throughput will make near-real-time testing practical.

Toward a Foundation of ATR Theory

Approaches to ATR have typically involved variations on basic methods that can be categorized into the following three classes:

- Matched filtering,
- Pattern recognition, and
- Model-based vision.

Matched filtering is the most common approach, and the most successful at this time. Matched filtering is based on the equation $\|f-g\|^2 = \|f\|^2 + \|g\|^2 - 2\langle f, g\rangle$, so that an image f can be compared to a template g by computing the inner product $\langle f, g\rangle$ and normalizing by bias terms. By computing many inner products and finding a best fit among a large class of possible targets, a best-target hypothesis is determined. Of course, different templates are needed for different views and operating conditions. Translation invariance can be obtained by computing convolutions in place of the inner product (effectively computing the inner product at all possible translations positions), whereas rotation invariance has to be built in using multiple templates.

Pattern recognition is based on segmenting the signal data, to extract the target region, and then making measurements of that segment. Typical measurements involve area and shape features. The vector of measurements describing the segment is then compared to prestored vectors defining target classes. A difficulty with pattern recognition is the dependence on the segmentation.

Model-based vision uses a geometric description of the target classes, in such a way that a description can be quickly generated based on any hypothesis or the position and orientation of a given target. The description, rather than being a vector of measurements of a single segment, is more typically a collection of unordered features representing significant events in the data that are likely to be extracted in a view of the target.

These three methods have more in common than is at first apparent. It is possible to unify the approaches in a single theory, which provides for increasing sophistication of each of the three methods. Indeed, one formulation of a model-based vision provides a matched filtering interpretation, where the filtering takes

place in a feature space. At the simplest level, matched filtering makes a comparison between an observed scene and a stored model of a target. By repeating the comparison at all positions, with all possible poses of the target, over all targets of interest, a best fit can be found. The comparison can be made based on the relationship of intensity levels in the image to predicted intensity levels, but it is more common and more robust to use image features that are less sensitive to natural variations. For example, extracting edge maps, and comparing observed edges against predicted model edges, can provide recognition that is less sensitive to the overall intensity of the image. With SAR imagery, it is usual to extract peaks, target, shadow, and background pixels, and to compare iconic images at the symbolic level.

Improvements are possible by extracting and grouping features from the sensor data that provide more localized, independent information. For example, whereas edge information provides useful discrimination power, groups of edges can be clustered to form line segments, or curves, that can be described by a few succinct parameters per grouped edge. Apart from providing more compact representations, the grouped information provides opportunities for more accurate reasoning about the components of the image, and the likelihood that the independent groups form an instance of a target. Methods for grouping raw sensor data into clusters of independent meaningful localized features will be dependent on the sensor type, the kinds of target models, and the ingenuity of the researchers.

The benefit of a foundational theory is that the needs and requirements of the system can then dictate design considerations, rather than the other way around. Indeed, there is a pressing need to be able to predict and assess likely performance according to operational conditions, sensor resolution, and target variability. Performance prediction then allows the development of sensor resolution requirements. The goal is to graduate ATR development from tinkering with demonstrations to development of advanced systems.

Domains of Applicability

Current ATR algorithms, such as the feature comparison algorithms mentioned above, are able to perform reasonably under the following assumptions:

- Targets must be unobscured and in the open;
- There are no more than a dozen or so target types, and the targets demonstrate relatively little intraclass variability between instances at the same orientation;
- The platform cues the system with certain imaging parameters, such as depression and squint angles; and
- The adversary does not employ significant cover, concealment, and deception (CC&D) techniques.

These assumptions represent necessary constraints because current ATR systems can only deal with a limited number of potential hypotheses at each location. Even with these undesirable limitations to their capability, ATR systems are still potentially significant in a variety of military applications. Although there are no fielded systems, the feasibility of deploying ATR systems has been demonstrated through the use of multistage methods of comparison of system features with prestored models.

In order to extend the applicability of ATR systems, further performance improvements are needed for operations in more challenging environments. For example, future ATR systems will be required to make accurate determinations regarding possible targets that are articulated, or that are partially obscured. This capability is more profound than it may at first seem, because it is not possible to enumerate all possible articulations and all possible partial obscurations as individual and separate models. Not only does the number of models grow exponentially, but the cross-talk between models also becomes large, and the ability of the system to discriminate among competing hypotheses becomes difficult. Instead, it becomes necessary to reason about subparts of a model, each of which might be recognized only indistinctly, but which, in conjunction, might form strong evidence for the presence of a potentially deformed or modified target. In order for ATR systems to operate effectively in the complex combat environments that are likely to characterize future naval engagements, they must be capable of analysis and recognition in the face of uncertainty and partial evidence. They must be capable of creating and utilizing combinations of data and must be able to take into account dependent information. Such capabilities may be within reach and, if so, will lead to ATR systems capable of operating in complex and variable combat environments.

In many parts of the world, military vehicles and other targets of interest will operate in wooded regions under foliage, or be otherwise hidden from the view of normal optical and radar sensors. Foliage-penetrating radar can help image targets under these conditions, usually at the expense of resolution because the bandwidth of the radar signal becomes limited. Preliminary studies indicate that considerable progress is possible at penetrating a layer of canopy. Further, foliage cover, as well as netting, often hides a target from many aspect angles but leaves open the potential for recognition at particular viewing angles. Accordingly, it becomes necessary to collect and integrate information from multiple viewpoint directions, as well as from multiple sensor platforms. Platoons of unmanned surveillance platforms, such as UAVs, will need to cooperate and coordinate in examining regions of interest in difficult terrain. Once again, technology that reasons about multiple pieces of uncertain evidence becomes critical to a fully functioning system. Such semicognitive capabilities are certainly realizable but require advances over current customary computational practices.

The ability to image and recognize moving targets is another key capability that will be required of future ATR systems. Certain targets, such as mobile

missile launchers, are visible while in transit. Current SAR techniques are only effective in imaging fixed targets. A nonmoving target is required to coherently deconvolve and sum the return signals from probing radar beams emitted from a range of aspect angles relative to the target. If the target moves with an unknown motion at the same time that the platform is moving, the disambiguation process becomes seemingly impossible. It is, of course, possible to obtain a measure of the motion of a potential target by observing and tracking the Doppler shift, but currently fielded systems provide no information about the potential target other than an indication of the motion. Alternatively, ISAR techniques allow for the imaging of moving objects (with uniform motion) by a fixed sensor.

Algorithmic techniques that re-register the information based on methods related to auto-focusing show promise for enabling radar-based ATR systems to obtain resolution on moving targets. Such highly specialized signal processing methods require nurturing and development, and considerable experimental validation, and tend to require nontraditional thinking about the image formation and signal processing theory. It is expected, however, that imaging of moving targets will become a viable technology. Such a capability could be extremely powerful, since the speed, direction, and pattern of movement of a target provide considerable evidence of the mission of the object, as well as constraints as to the orientation and variability of the target. Together with a few distinguishing features on the oriented target, full identification becomes much more likely due to the motion analysis.

Temporal integration of information also offers powerful potential but has been largely untapped for ATR processing. For example, in automatic mine detection, land mines that are placed sufficiently far underground can fall into the "too hard to detect" category soon after placement. Suppose, however, that a small collection of vehicles is observed positioned on a field in a particular pattern, and that a half year later, an explosion yields evidence that there are buried mines in the field. Correlation of the information of the single explosion with the position of the suspicious vehicles at the earlier time can lead to determination of the location of the remaining mines. Such simple and obvious techniques nonetheless require large storage capacity, and the ability to retrieve seemingly trivial data. This ability to bring into correspondence multiple pieces of information, often separated temporally, with terabytes of information juxtaposed in between, offers formidable challenges that nonetheless promise great advances in our ability to recognize and reason about targets. Such information understanding, which extends beyond that enabled by simple ATR capabilities, is the topic of the section below titled "Information Understanding."

Performance Estimation

There are two ways to estimate the performance of a proposed target recognition system. One is to build it and test it on a large database of acquired images, and to evaluate the performance. Another method is to analyze the algorithms,

using simulations, with an emphasis on the discriminability of the models, to determine, before actually building the system, if the method has any chance of working. Current practice is closer to the former methodology than to the latter.

It is possible to predict the performance of ATR systems by measuring performance statistics associated with the underlying features used for the recognition process. Even if a system makes use of complex combinations of partial evidence from competing models and operates in a hierarchical indexing fashion, it is nonetheless possible to determine the likely degree of overlap between configurations of targets, which can vary due to sampling and extraction uncertainty as well as in-class variability, and competing configurations, which can occur from random clutter and background or from competing models. Models of the variability of the features are needed in order to perform this analysis, and it is often necessary to assume that the features are independent. However, it can be quite useful in development to know how much information is required for an ATR system to perform at an acceptable response operating level, before actually building the complete system.

Consider as an example a two-class problem, where there is a single target type such that all locations in the image domain are to be identified as either target or background. A target is indicated by the presence of a collection of features and a specified percentage of the designated features will actually be present and extracted when the target is actually present. There is a statistical variability to the number and quality of these features, and so the total score indicating the presence of a target has a certain density function when the target is actually present. On the other hand, when the target is not present, random noise and other potentially confusing elements will cause patterns of features to be present with certain probabilities, and so there is also a density distribution for the total score for a target when the target is not present. By adjusting the threshold on the score, different operating points can be obtained so as to vary the expected detection rate versus the false alarm rate. The entire operating curve can be predicted if the density distributions of the scores can be computed. Computation of these curves requires a statistical analysis of the properties of the features, with and without a target being present, and requires either independence of the features in the two cases or an understanding of the joint statistics.

Generally, a certain number of independent features are required to enable discrimination between targets and background. In one kind of sample analysis applied to a simple image processing example, a 90 percent detection rate with a reasonable false alarm rate (one per kilometer) is possible only when there are features defining the target with an aggregate of 35 coordinate values. Different assumptions lead to different requirements, but these results are typical. Since features are rarely completely independent, the estimate provides a lower bound for the requisite number of features. A feature can be a component or measured attribute, generally associated with a location in the image, based on extraction and grouping of particular patterns of intensities or edges. For example, the

opening angle of a corner is a feature associated with detection of the corner and can be used to assist in discriminating between the particular corner in question and a corner to be matched in a model. If it is determined that 30 to 50 features are required in order to perform reasonable discrimination (i.e., keeping the detection rate high without incurring an unreasonable number of false alarms), then the estimate implies certain resolution requirements for the image acquired by the system. A critical quality measure is the number of pixels on target that are extracted from the sensor data. Whereas typical imaging systems provide sampling rates of 1 pixel per 2 feet, or per single foot, resulting in 100 or so pixels lying on a typical target, it might well be the case that in order to obtain 50 features about a target, 500 pixels are necessary. The extra pixels might come from multiple views, or from multiple sensors, or from improved image formation and ultrahigh-resolution images. The important point is that a well-developed theory of discriminability can provide resolution and sampling requirements, which can greatly assist in the development process.

Indeed, although ATR is an extremely challenging problem that often involves identifying targets in a complex and highly variable environment with multiple levels of CC&D, it is the panel's expectation that significant evolutionary progress will be made. The advances in sensors, resolution, processing capability, and algorithms that conduct reasoning in the face of uncertainty will likely enable discrimination among dozens of target types, under conditions of partial obscuration and other challenging conditions.

INFORMATION UNDERSTANDING

Information understanding involves the fusion of data that may be spatially and temporally distributed in order to form a coherent picture of a situation of interest. Information understanding depends on the ability to recognize and extract relevant data from large and disparate data collections—extracting useful information from large sets of redundant, unstructured, and largely irrelevant will often be the first step in developing information understanding. In the commercial world, current extraction techniques utilize data mining.

Data mining, which has potential DOD applications, currently focuses on the need of credit card companies to automatically recognize spending patterns that indicate probable fraud, based not only on current purchases, but also on the extent to which the current pattern is unusual for the card in question. Other business uses of data mining and collaborative filtering include profiling of potential customers based on their spending patterns, so as to target marketing efforts to the most likely consumers of products and services. Since the marketplace rewards businesses that can exploit a comparative advantage, data mining tools for business applications will inevitably become an important part of mainstream commerce. In medical data processing, there is the possibility of developing automated diagnostic procedures that identify conditions or pathology from

multiple test results. Defense needs are conceptually similar, but broader and different in scope—information relevant to national security can be extracted from nearly all information sources. Further, rather than focusing on securing a competitive advantage in sales and marketing of goods and services, defense needs include more general intelligence, indications, and warnings, and other information that can facilitate combat planning and execution.

Information understanding technologies to meet defense needs may draw upon the same underlying theory that supports commercial information extraction techniques, but generally will require a different set of applications. Currently, ATR can be viewed as a primitive form of information understanding technology, which should ultimately lead to battle-force analysis and automated situation awareness, and all-source automated multisensor analysis. The development of these capabilities will be driven by user needs and will be facilitated by advances in sensors, communications, and computation.

Recognition Theory

Recognition theory refers to the body of knowledge underlying the development of tools for extracting information from large and varied data sets and is the underlying foundation of those technologies that are referred to in this report as information understanding. The theory of pattern recognition, which involves the identification of distinctive patterns in signal data, is a special case of recognition theory. Typically, pattern recognition uses a single image or a single return signal and attempts to distinguish among a fixed collection of possibilities in order to characterize the given data. More broadly, recognition theory encompasses systems with greater cognitive processing capability that are flexible enough to effect recognition in the context of situations and scenarios that have not been explicitly programmed into the recognition system. Further, recognition theory should enable the development of systems that can discover associations among disparate pieces of information.

Methods developed in the field of artificial intelligence (AI), including commonsense reasoning, nonmonotonic logic, circumspection, algorithms used in neural networks, and extensions to Bayesian calculi, have largely failed to provide the understanding required to develop a coherent theory of generalized recognition. Accordingly, recognition does not yet exist as a differentiated discipline. However, given the ongoing progress in AI research, the panel anticipates that a coherent theory of recognition will emerge. Further research and development is needed to develop the capacity to reason in the face uncertainty and to fuse information from disparate sources.

Automatic target recognition uses recognition theory in limited ways. Most ATR development is currently limited to the pattern recognition subset of recognition theory, being based on analysis of single image frames and segmented target regions. However, more generalized ATR processing would take advan-

tage of multiple geo-registered information sources and temporally displace data in order to dynamically reason about situations.

One of the main differences between the theory of pattern recognition and more general recognition theory is summed up in the standard distinction between bottom-up and top-down processing. Recognition theory seeks a solution to the problem of identifying and extracting information that is relevant to a particular working hypothesis from large and highly varied sets of data. Since extraction and analysis are driven by a hypothesis, recognition theory can be viewed as largely top-down processing. Currently, most recognition systems work in a bottom-up fashion, first extracting features from the given sensor data, and then looking for patterns among the features that support a model hypothesis. Although hypotheses are formed in the course of executing pattern recognition, it is the sensory data that largely dictates the flow of processing, and bottom-up processing is the more appropriate description for the information flow. When data sets become too large to carry out bottom-up processing, and when information must be extracted from multiple and highly varied sources, processing methods necessarily must use analogs of inverse indices and top-down processing.

The Future Information Environment

The panel assumes a future in which sensors and information will be ubiquitous. Encryption will be used to protect certain vital information, such as bank transactions, but massive amounts of other information will be available for analysis. Not only will personal and official messages be passed digitally, but every appliance will also be communicating by networks with remote controllers, and every individual can be expected to be in constant contact with a vast interconnected digital network. Highway tolls will be paid electronically, and packets containing information as to the whereabouts of any moving private vehicle will likely be available. This sea of information will include data about individuals from government and commercial sources. It is reasonable to assume that the whereabouts, movement, purpose, and plans of most individuals will be discernible from an analysis of specialized information, and that most businesses and companies will have massive incentives to perform such analyses in order to target their marketing to the appropriate potential customers. Although encryption of the information may afford some privacy to individuals, analysis of data traffic patterns may provide nearly equivalent information, at least in a statistical sense. To the extent that information can be captured, it can also be archived, and it is anticipated that a massive, distributed, dynamic database of archived information will be developed specifically for Navy and Marine Corps needs. The technology that will be developed to analyze and exploit the sea of information that will be available in the future will pose both challenges and opportunities for the DOD and the Department of the Navy.

In the same way that the needs and plans of an individual potential customer can be analyzed, so also can the plans and movements of potential adversaries be observed. Armies are made up of individuals, and commanders begin operations by setting plans and positioning people and materiel. National security will dictate that all appropriate sources of information be acquired, monitored, and assessed. The key to these capabilities is the ability to understand the information in ways that are relevant to particular needs. Understanding and managing information will be critical to defense needs.

ADVANCES NEEDED TO SUPPORT INFORMATION UNDERSTANDING

While much of the research that is required for the development of technologies to support information understanding is currently ongoing, in the view of the panel, it is not sufficiently focused on developing information understanding applications for Navy and Marine Corps needs.

The panel has identified the following six technology areas as meriting special attention in order to realize the information understanding capabilities that will be required to analyze and exploit the sea of information that will characterize the future information environment:

1. *Information representation*. Information representation involves extracting and representing features from data streams in such a way that the relevant information can be accessed efficiently from automated queries. Methods of information retrieval likely will include inverse indices and distributed processing using intelligent memory. It will be necessary to develop the means to appropriately represent information without prior knowledge of the likely hypotheses that might later be used to extract the representation or to associate other data with it.

2. *Information reasoning*. Information reasoning involves the capacity to reason in the face of uncertainty, and may include the use of models to predict degrees of dependence and independence between data sets and other strategies in order to effectively hypothesize and test premises for the purpose of extracting relevant information content. Further advances in recognition theory are needed, including methods for combining data and forming inferences. Recent developments in neural network theory suggest that it may be possible to create adaptive reasoning systems, but further advances are required before such systems can be realized.

3. *Information search*. Since information understanding will most likely work with a top-down structure, methods are needed to organize hypotheses hierarchically, in order to structure the search for content logically and efficiently. In the same way that model-based systems generate hypotheses that are verified and refined in a tree-search structure, analogs are needed to organize the search for information content. Further, the search cannot be hand-crafted for

each recognition system application. Instead, methods are needed to automatically generate the search trees and hypothesis organization strategies.

4. *Information integrity.* Because data might be corrupted, faked, or inaccurate, not all information sources should be trusted equally. While technologies exist for authenticating information and securing its transfer, means of assessing confidence in information sources, and the ability to discard untrustworthy information, are topics that need further development.

5. *Information presentation*. Information presentation, as opposed to representation, is the manner in which processed data is supplied to the human operator or commander. This involves the human-machine interface as well as the specific manner in which the data is displayed and its context established. Capabilities for data visualization and multimedia presentation of information will be important for the best performance of an information understanding system that necessarily includes a human operator as an integral subcomponent of the system.

6. *Human-performance prediction*. An information understanding system that includes the human operator as the final arbitrator and decisionmaker can be effective only if the human-machine interface is optimized with respect to human performance in the context of the task at hand. Accordingly, it will be necessary to acquire greater understanding of human cognition and decisionmaking behavior.

Because information understanding is a cross-cutting endeavor, other technology enablers in addition to those listed above will play a role in its realization. For example, networking technology, including data transfer and connectivity standards, will be an important factor.

SUMMARY

In the future, sources of information will include DOD organic systems, systems from other government agencies, emerging space-based and airborne commercial imaging systems, other commercial information providers, and public-domain sources that will emerge from the burgeoning information infrastructure.

As information becomes increasingly central to commerce, society will move from an environment of relative information scarcity to one of information abundance, in which applications must locate and correlate information from massive sets of seemingly unrelated data. Technology development is required to develop the applications that will effect the transformation of raw data to higher levels of information understanding, which will include not only the extraction of fixed patterns from sensor data, but also the analysis and reasoning about correlations and co-occurrence of relevant observations. Current applications typically perform pattern recognition on real-time data collected by dedicated sensors; future information understanding systems will need to perform higher-order reasoning about information from the full range of available information sources.

4

Advanced Sensors

INTRODUCTION

A major theme of this report is the revolutionary impact of information technology emerging from the commercial sector on the prosecution of military operations. Advanced sensor technology is a crucial element of information collection, and one example of an evolving commercial business area with obvious military applications is airborne and particularly space-based image collection. In the near term, new ventures in this area will offer affordable submeter-resolution panchromatic as well as colorized imagery of most areas of Earth from commercially launched space platforms. Details of these enterprises are provided in Appendix C. In addition to providing new services and products, this industry will drive the development of low-cost, lightweight advanced sensors that will have spin-offs for uniquely military applications.

In spite of the major contributions the commercial sector is likely to make toward satisfying future military sensing requirements, there will always be a subset of those requirements that has no identifiable, profitable commercial counterpart. This chapter explores some of the sensor technologies that will be critical for future military operations, many of which will require DOD and possibly Department of the Navy investment to ensure their robust development and tailoring to naval applications. The focus here is on standoff sensors such as radar and electro-optical systems, which will be the workhorses of future reconnaissance and surveillance platforms. These platforms are expected to be under the control of the Joint Task Force Commander and will provide the information necessary to conduct naval missions and operations. The Department of the Navy must ensure that it provides connectivity to those assets provided by other Services or the National

community, and invest in organic sensors and platforms to meet unique Navy Department requirements that will not otherwise be satisfied. The issue of sensor platform types is also discussed, since the requirements on these platforms are often intimately tied to the capabilities of the sensors they carry.

RADAR TECHNOLOGY ISSUES FOR FUTURE NAVAL WARFARE

Introduction

Warfare in the future will become increasingly dependent on technological force multipliers as the numbers of personnel and equipment shrink in response to economic pressures, and as adversaries avail themselves of similar capabilities available in the open marketplace. Surveillance and reconnaissance are two military capabilities that will undergo dramatic growth in performance as a result of the explosion in information technology. Processing technology will enable surveillance coverage rates that are orders of magnitude higher than those achieved today. Wide-band communication via satellite or terrestrial channels will provide surveillance products on demand to warfighters in the field, who will be provided with the data storage and the tools necessary to take advantage of them. As military commanders seek near-perfect knowledge of the battle space in which they fight, it is critical that both the capabilities and limitations of these technologies be well understood as we postulate sensors and systems that might exist decades in the future. In all cases, it is necessary to assess such future capabilities in terms of their military utility to find, identify, and prosecute targets of interest to the forces.

To fully appreciate the role of reconnaissance and surveillance on the future battlefield, it is also necessary to extend the several "system of systems" concepts that are emerging as part of the current revolution in military affairs. One such concept is surveillance/precision strike, seeking the seamless integration of emerging highly accurate sensor location systems with the new precision-guided weapons based on GPS, terminal seeker, or other guidance concepts enabling hit-to-kill accuracy in the end game. A second example is the automatic fusion of real-time sensor and intelligence data in the context of various geographic and intelligence preparation-of-the-battlefield (IPB) databases to find and identify individual critical mobile targets such as the Scud transporter-erector launchers (TELs) that caused frustration in the Desert Storm campaign. Each of these needed capabilities suffers today from shortfalls in either basic sensor technology or exploitation technology. Many of these shortfalls will gradually disappear, but some limitations will remain due to physics-based limitations or cost constraints.

Platform Issues

A major issue for the future of reconnaissance and surveillance is the types of platforms in which the Services, and in particular the Navy, should invest.

General categories are space-based, airborne, and shipboard, the latter including both surface and subsurface platforms. A significant focus of this chapter is littoral operations, with particular emphasis on force projection ashore, whether for major regional contingencies, special operations, or operations other than war. Since most such operations will require deep look capability into hostile territory, the major platform competition in the future will be between spaceborne and airborne assets. Secondarily, there will be a competition in the airborne category between organic carrier-based assets and land-based assets within the inventory of the Navy or one of the other Services. Each of these surveillance platforms has its own set of advantages and disadvantages that must be fully understood and weighed against one another to arrive at a reasonable strategy for technology and system investment.

Many people believe that space is the ideal place to put most of the surveillance and reconnaissance assets in the long run. The reasons are many. First, space provides a vantage point from which no point on Earth is denied to a sensor system. Airborne assets are usually required by international law to fly over friendly territory in the absence of an outbreak of hostilities, and in most cases must do the same under wartime conditions out of consideration for safety. In fact, wartime conditions usually drive airborne platforms many tens of miles further back from the front once hostilities begin. As a consequence, airborne sensors are significantly limited in their ability to see deep into enemy territory—active radar sensors because of limitations on power versus slant range, and passive imaging sensors because of loss of spatial resolution due to limited angular resolution. Although these effects are suffered to some extent by both airborne and space-based sensors, airborne sensors are subject to the increasingly deleterious effects of atmospherics and weather as grazing angles become shallower, and sensors that must look at surface or low-flying targets become increasingly screened by terrain masking in theaters such as Bosnia or Korea. By maximizing the grazing angles over which it deploys its sensors, a space-based system minimizes the amount of atmosphere its signals must pass through, and suffers virtually no shadowing effects due to mountains. A doctrine of military intelligence existing from time immemorial is to seize the high ground so as to see the enemy, and clearly there can be no higher ground than space.

A second advantage argued for space-based sensor systems is that once the nonrecurring cost of producing and launching the sensors has been paid, the continuing infrastructure cost of utilizing the sensor is dramatically less than that of large airborne surveillance platforms. This argument no longer applies exclusively to space-based platforms, however, because the same case can be made for the evolving UAVs and for proposed future uninhabited reconnaissance aerial vehicles (URAVs). An advantage of a space-based system over the URAVs, however, is the high survivability afforded by the platform against potential enemy attack. Since the cost of developing and fielding antisatellite weapons will be prohibitively expensive and will require a high degree of advanced tech-

nological capability, only the most sophisticated of potential future adversaries will threaten such platforms. A more likely threat to space-based sensors will be electronic countermeasures and other techniques of information warfare, including camouflage, concealment, and deception (CCD).

On the negative side of the argument for space-based sensors is the issue of nonrecurring cost. The special environmental conditions in space obviously drive costly hardware solutions to meet temperature, radiation, and low-operating-power requirements, as well as the mechanical constraints associated with launch stress and foldability of the payload into the launch vehicle. The unique requirements of surveillance itself, moreover, can be significant cost drivers, depending on the level of performance sought. For example, if near-continuous coverage of an area on Earth is required, the choice is generally between one or a few satellites in synchronous orbit and a large constellation of low-altitude satellites such as those being implemented for cellular communications. But if an active radar sensor is required, the option of having satellites in synchronous orbit becomes prohibitive due to the R^4 dependence of radar signals on target range. Even a radar sensor in low orbit suffers from R^4 dependence, since practical considerations of orbital decay require significant satellite altitude, which maps into slant range requirements at least as severe as those of airborne radars, and typically worse. As a consequence, depending on the nature of the surveillance requirement, even a low-orbiting system may have to carry a very expensive radar sensor. For many tens (or hundreds) of such satellites, the nonrecurring bill could be quite large. Examples of requirements that may fall in this category are wide-area moving target indicator (MTI) surveillance of ground targets and airborne early warning (AEW) radar surveillance in support of theater missile defense. In general, providing surveillance for moving targets strains the ability to field affordable radar solutions from space because it requires a high revisit rate for near-continuous coverage. Fixed-target imaging systems in space, on the other hand, have been tremendously successful since the required rate for revisiting a given point on Earth may be much lower. Even active imaging systems are more cost-effective when the target is fixed, because they are able to use long integration times for coherent image formation at the desired resolution, with the side benefit of being able to operate with much lower radiated power than short-dwell active systems.

The primary alternatives to space-based surveillance systems are various categories of airborne platforms. Typical of today's land-based airborne surveillance systems are big platforms such as the P-3, the E-3, the E-8, Rivet Joint, and others. Other platforms include the carrier-based E-2C, as well as a variety of smaller signal intelligence (SIGINT) and other special-purpose platforms such as Guard Rail. A major issue to be considered for the future is the place of carrier-based versus land-based surveillance. As the Navy transitions to a posture of littoral operations and force projection ashore, the case for organic platforms versus land-based support is weakened. Furthermore, the concept of joint

warfighting argues that the surveillance assets of the other components will be available to support Navy and Marine Corps forces when required. On the other side of the coin, the number of foreign bases from which these joint assets may stage is diminishing at an alarming rate, and it is not clear that many of these platforms will have the "legs" to reach certain theaters of operation. One potential solution to this problem is the deployment of long-endurance surveillance UAVs, for which the model in today's technology might be the Defense Advanced Research Project Agency's (DARPA's) Global Hawk (Tier-II+). With future, perhaps larger versions of such platforms, it should be possible to carry large surveillance payloads to the fleet from thousands of nautical miles away, loiter in the operating area for one or more days, and then return safely to the originating base when a relieving platform arrives on the scene. In the near term, land-based airborne surveillance will continue to be dominated by large manned platforms, and the Navy and Marine Corps should provide the appropriate data links and connectivity to these platforms so as to benefit from their presence in joint operations.

The Department of the Navy should also evaluate and potentially develop organic surveillance assets that would be attached to the carrier battle group for those circumstances in the early phases of a conflict where naval forces are first on the scene and do not have the necessary surveillance of the littorals required for the projection of power ashore. Such an organic asset could provide surveillance over land to ranges of 50 to 100 kilometers prior to the appearance of joint airborne or UAV assets in the theater of operations.

In the long term, the concept of URAVs is certainly technically feasible and will soon be demonstrated in near-term ACTDs. The total operational concept for the deployment of such surveillance systems must, however, be thoroughly understood. For example, the classical problem of providing radar surveillance of ground or airborne moving targets usually requires a radar with a certain power-aperture product in response to a requirement for target radar cross section and slant range. Since this requirement varies as R^4, the size of the radar, and hence of the platform, increases very quickly with separation between radar and target. To satisfy the requirement with a small UAV carrying a limited payload (e.g., the total Tier-II+ payload is 2,000 lb), it may become necessary to penetrate enemy territory to achieve the necessary slant range for target acquisition. Against a strong adversary, this approach may impose a requirement for low observability on the vehicle and its sensor package. In addition to the cost of designing and maintaining a stealthy penetrating vehicle, another factor comes into play. As the vehicle is forced to penetrate enemy territory to overcome the R^4 disadvantage, the radar emissions themselves compromise the survivability of the platform. Thus low probability of intercept (LPI) may have to be added to the requirements of the radar design, which may have a significant impact on range performance. It is not clear where the regression ends here, particularly as it affects the cost of the surveillance system as well as its net performance. An alternate solution is to

place a much larger radar sensor with a large power-aperture product at standoff ranges from the enemy's defenses so as to afford a reasonable level of survivability, as well as the radar "horsepower" needed to perform the mission at much longer range. In this case, system designers typically choose a large platform to provide the lift, power, and cooling necessary to support the sensor. Given the large platform, the tendency has been to populate the aircraft with large crews to support and exploit the system's full capabilities on board.

There is a tendency to view the large platform solution that is common in today's surveillance inventory as being driven by the on-board exploitation requirement. In fact, the size of the sensor may be the more fundamental driver. In the future, it should be possible to combine these two modes of surveillance by having much larger unmanned or lightly manned platforms capable of carrying standoff radars, but without putting so many people in harm's way, and without the expense of training and deploying large, highly trained flight crews. Wideband, secure satellite or point-to-point communications will enable near-real-time reconnaissance and surveillance to be done wherever the commander would like, and automated flight control systems together with telepresence will permit large URAVs to replace manned standoff platforms in the future. Such platforms will be able to interoperate with small, stealthy penetrating UAVs carrying passive sensors or active LPI imaging sensors. A standoff ground surveillance system could provide high-quality wide-area moving target detection, location, and target development, tasking the small systems to provide positive target identification based on cues from the "mother ship." The small systems could also complement the coverage of the standoff platform using LPI "spot mode" moving target indicator and synthetic aperture radar capability, together with intermittent operating protocols, to provide survivable focused surveillance of small areas, such as those screened from the large URAV by mountains. When cued by intelligence information to a narrow search area, this mode of operation could also be used to find deep targets out of range of the standoff system. Such a configuration of large standoff URAVs supported by constellations of small penetrators could provide the target development necessary for weapon delivery systems such as the arsenal ship and submarine-launched ballistic and cruise missiles, as well as for today's shipboard and airborne weapon delivery systems.

Key Radar Technology Areas

Radar technology development is likely to continue its evolutionary pace over the next several decades. Advances in solid-state transmit/receive (T/R) modules will include higher output power, greater direct-current-to-RF conversion efficiency, and increasing miniaturization. Even more importantly, costs will drop dramatically as production volumes increase, leading to extensive use of this technology in future systems. This will enable a variety of active array designs with two-dimensional electronic beam steering and dynamically

reconfigurable apertures that will optimize multimode radar performance. Multipolarization and multifrequency shared apertures will enhance the information gathering capabilities of future systems for such purposes as target classification, and will aid in the rejection of various sources of clutter. Large apertures processing wide instantaneous bandwidth signals at large-scan angles will be enabled by photonic manifold technology or by direct digital techniques. Fighter radars will exploit T/R module technology to provide a variety of sophisticated air-to-air and air-to-ground modes, both detection and imaging. Higher average power achieved will enable fire control solutions at very long range against conventional targets, and will begin to have benefit against small-cross-section threats. Ship-based air defense radars will see a similar benefit in enhanced sensitivity as well as flexibility in the prosecution of multiple simultaneous fire control solutions.

Exciter and receiver technology will achieve increasing levels of stability, permitting the detection of small moving targets in very-high-clutter backgrounds. As analog-to-digital converter technology improves in both sampling rate and dynamic range, more receiver functions will be performed digitally, leading to precise control of receiver characteristics and channel matching. Many antenna designs will exploit multiple subarrays on receivers to enable a variety of array signal processing techniques to be applied. Space-time adaptive processing (STAP) of digitally equalized subarray channels will provide unprecedented levels of MTI performance. The ability to form multiple simultaneous (or near-simultaneous via pulse interleaving) beams will permit SAR images of multiple areas to be created in a single coherent collection interval. Ultimately, particularly at lower RFs, conversion to digital signals may occur at the output of each T/R module, leading to all-digital array manifolds and receivers. Achievement of this long-term goal will provide the ultimate in flexibility for array processing, with the most sophisticated of algorithms possible, provided that a sufficiently powerful signal processor is available.

The radar signal processor will be the most critical element in any sophisticated radar of the future. The tendency to exploit COTS solutions involving massively parallel configurations of high-performance processors will continue. Processing systems with teraflop levels of performance will be employed for radar signal processing, tracking, and target identification algorithms. Algorithm design and signal processing software development will be areas of increasing focus, with sophisticated graphically based development tools providing rapid prototyping capability. Similarly, detailed control and dynamic reconfiguration of radar will become increasingly software dominated, with the hardware elements tending toward programmable universal smart modules with embedded processors capable of a wide range of performance when commanded over digital control buses.

Several radar system concepts may reach maturity over the next several decades. Bistatic radar has held much promise but has been hindered by imple-

mentation difficulties and a lack of well-defined concepts of operation. Hybrid systems involving spaceborne radar illuminators and stealthy UAVs carrying bistatic receivers and signal processors may prove their military advantage in hostile environments. Similarly, the bistatic exploitation of existing signals in the environment may lead to practical low-cost radar detection or imaging equipment. AEW systems using the lower RF bands together with STAP processing will permit the detection and tracking of low-cross-section aircraft and missiles. In radar imaging, SAR image resolution will continue to improve within limits imposed by atmospheric distortion. Advances in autofocusing techniques will likely extend the ranges at which these higher resolutions can be achieved, and operational microwave SARs with several-inch resolution should be achievable.

The explosion in digital processing technology will provide great benefits in reducing the vulnerability of radars to electronic countermeasures (ECMs). Electronically scanned arrays together with sophisticated algorithms will be employed to sense the jamming or casual interference environment in time, space, frequency, and polarization dimensions, adapting the radar's operation in real time to changing conditions. Spatial/temporal adaptive cancellation algorithms will not only provide greatly increased levels of performance against conventional sources of direct interference, but will also be effective against airborne jammers employing terrain-scattered signals. The use of T/R modules will provide very wide radar operating bands, making frequency agile radars more effective against moderately sophisticated reactive countermeasures.

Sensor Exploitation Issues

One of the weakest links in current sensor-to-shooter concepts is the capability to derive classification or identification information from sensor data. If lighting and weather conditions permit the collection of high-resolution optical imagery of a target complex, human operators and increasingly powerful machines can provide highly reliable classification of selected targets, but wide-area high-resolution imaging requires a high degree of automation. Electronic intelligence (ELINT) collectors can frequently provide precise classification of signal-emitting complexes based on the unique signatures observed. The most reliable long-range all-weather sensor is radar, however, and the state of the art in this realm is by no means complete. A great deal of investment has been made in automatic classification of targets seen in SAR imagery, and a certain degree of success has been achieved against certain targets in the clear. Much is left to be done to achieve robust classification at low false alarm rates for targets partially screened by foliage or other obstructions, and targets deliberately camouflaged by an enemy to defeat the classifier. As sensor resolutions improve, yielding more pixels on target, and as processing technology continues to advance at its rapid pace, enabling more sophisticated algorithms to be employed, the performance of the classifiers will improve steadily, and should provide a very power-

ful capability over the next several decades. This applies primarily to the microwave region SAR systems. At the low end of the RF frequency band, ongoing research is trying to achieve foliage penetration (FOPEN) and ground penetration (GOPEN) SAR imaging systems capable of finding and classifying obscured or buried targets. In contrast with the microwave SAR, these systems suffer from a fundamental conflict between the desire to utilize the lowest RF possible so as to achieve maximum penetration of the obscuring medium and the desire to maximize RF bandwidth to achieve high-resolution images. This area of investigation should converge to some optimum balance between mutually exclusive requirements, and the performance may not improve further beyond that point. Nonetheless this technology may provide great military value based on modest levels of classification performance.

The collection capability of future SAR systems will result in astronomical quantities of imagery at very high resolution. The fundamental limitations on SAR collectors today are not the sensors themselves, but the signal processors necessary to generate imagery and the data links necessary to disseminate it. Both of these limitations will all but disappear in the coming decades, resulting in collection systems that will be capable of imaging entire theaters of operations at very high resolution daily, or even several times a day. Human operators will be relegated to examining imagery that has been highly screened by automated techniques so as to reduce the bandwidth to that which is manageable by a finite number of interpreters. The ATR problem of finding and keeping track of mobile targets will be greatly assisted by the use of automatic change detection applied to SAR and other imagery, and three-dimensional interferometric processing of multipass SAR imagery will add height to targets, providing another dimension of information to enhance ATR performance. Dual polarization and multispectral SAR augmented by multispectral passive imaging under benign weather and cloud conditions will further increase the information content for each target on which the ATR system will operate. In response to this pervasive fixed target surveillance capability, future enemies will engage in ever more sophisticated CCD techniques to evade detection. This will drive sensor and ATR developers into seeking ever-increasing capabilities from their systems to identify partially obscured or disguised targets. It is not clear today which side will gain the upper hand in the long run, but economics will ultimately be the governing factor.

A relatively embryonic area of radar exploitation is in the area of moving ground targets. Virtually all airborne or spaceborne ground surveillance systems are either imaging systems, or systems that exploit a target's own emissions. Consequently, there is very little knowledge in the surveillance community about the potential benefits of moving target exploitation, and almost no prior body of knowledge on the subject. Moving target exploitation comes in several flavors, starting with the knowledge to be gained from the basic scan-to-scan detection picture obtained from a wide-area airborne ground surveillance system. Future MTI systems will have very high revisit rates on the order of once every few

seconds over very large areas (e.g., 50,000 square kilometers). These systems will have high-power-aperture products to achieve the rapid revisit rate, unaided circular errors of probability (CEPs) of a few tens of meters at extreme sensor range, and high single scan signal-to-noise ratio on individual targets to exploit unique signatures associated with rotating or other articulating parts of the target. The MTI modes will operate at very high range resolution so as to measure the length and down-range radar cross section (RCS) profile of each moving target, providing a one-dimensional crude ATR capability as well as a powerful vector association variable for maintaining track continuity. All moving targets will be automatically tracked, and individual targets will be aggregated into groups based on various rule-based filtering criteria. The RCS templating concept will be extended to groups of targets, enabling multiple hypothesis tracking algorithms to reacquire convoys hours after they have disappeared behind a mountain or driven into a foliage-obscured area. The ability to track each moving entity on the ground indefinitely will provide a mechanism for aggregating knowledge about that object over time, whether it is obtained from the on-board radar itself, of from off-board sources of sensor or intelligence data. The radar itself can be used to generate high-resolution ISAR images of selected targets as their track state is predicted to pass through curved road segments in the on-board geographic road network databases. These images, when classified by an ATR subsystem, would add to the knowledge base being built within that target's track file. Ultimately, the ability to indefinitely track and classify most moving objects on the ground together with intelligence data on the source and sink locations of vehicle movement should permit a complete dissection of the enemy's infrastructure, and ultimately yield a real-time ground order of battle. It will also provide a powerful mechanism for maximizing the utilization of narrow field-of-view sensor systems such as high-resolution spot SARs. Prior to an outbreak of hostilities, such a detailed analysis of the enemy's movement patterns should telegraph that adversary's intentions to intelligence analysts. In a peacekeeping mission, noncompliance with treaty obligations will be readily apparent in near real time as the movement of armaments and personnel is tracked throughout the theater.

Surveillance in Systems of Systems

The seamless integration of surveillance functions into an operational architecture for prosecuting a specific military mission represents a challenging systems engineering problem. Many of the architectures used in the past were developed on an ad hoc basis in response to an urgent need, and do not come close to optimizing the utilization of the various subsystems composing the architecture. The continuing revolution in the areas of information and communications technology will provide the physical basis for optimizing these architectures, but tremendous strides need to be made in developing and automating

viable concepts of operations for such large meta-systems. The development of these capabilities will require the coordination of large government and industry teams, both to create the new architecture and to engineer new interfaces for legacy systems to permit their incorporation into it. Considering the fact that a single major platform development by one prime contractor is a highly challenging engineering task, it is likely that the creation of a system-of-systems architecture will not be accomplished without considerable effort.

One example of such a desired architecture is surveillance/precision strike for near-real-time detection and identification of surface targets, followed immediately by their assignment in priority order to appropriate strike systems already in the field. This architecture would provide for the timely prosecution of moving ground targets, or mobile targets whose agility places their relocation period inside current planning cycles. Among the design challenges to be faced are the networking of surveillance, C^2I , and strike systems via appropriate digital communications, the prioritization of targets based on importance and vulnerability, the pairing of targets with appropriate weapons, and the dynamic positioning of forces to optimize system effectiveness. The surveillance component of this architecture must be designed to provide a sufficiently high number of viable target nominations per unit time to keep the strike component efficiently employed, with emphasis on finding the target types that are known a priori to be of highest military value. Since targets may be fixed or moving, both SAR and MTI radar capability must be employed. As described above, wide-area coverage will be possible for both radar modes, and technology will permit exhaustive SAR imaging of large areas in the future to match the wide-area MTI capability available today. The fusion of SAR change detection products and FOPEN radar products with MTI will provide a further enhancement to the long-term tracking of mobile targets.

A major challenge in the surveillance component of this architecture is the target identification problem discussed above. The degree of confidence required in the identification is a function of the particular scenario. In a free-fire zone presumed to contain only enemy combatants, the main concern is the efficient use of ordnance, and the allowable false identification probability may be somewhat high. On the other hand, for a decision to attack targets close to a battle area where ground forces are engaged, the acceptable level of error may be so low as to preclude achieving it with the state of the art in available radar sensor and ATR technology. In these instances, other sensors such as high-resolution electro-optical/infrared (EO/IR) or SIGINT, specific human intelligence (HUMINT) reports, or absence of the expected identification friend or foe (IFF) response may be required to reach a level of confidence necessary to shoot. In operations other than war, political considerations may be of overriding importance in deciding what level of identification is sufficient. If the goal of the surveillance/precision strike architecture is to achieve timely execution through automation of most functions, then the algorithms will need to be extremely sophisticated in order to

adapt to such scenario-dependent constraints. More likely, there will always be people in the loop to handle these tough questions. These operators will require rapid access to a great deal of information in as efficient a manner as possible so that they do not become the long pole in the tent for the targeting cycle.

ADVANCED ELECTRO-OPTICAL SENSING TECHNOLOGIES

Introduction

A number of enabling electro-optical phenomenological and sensing technologies will be important for future military applications. This section begins with a broad overview of the available technologies and then, for each, considers more specific platform basing and functional applications, including intelligence, surveillance, and reconnaissance (ISR), targeting, weapon delivery, and threat warning systems.

Enabling Technologies

Passive Multispectral and Hyperspectral Imaging

Over the last decade, it has become increasingly clear that color can provide significant information (of military value) for both manmade objects (targets) and natural backgrounds (clutter). Initial systems will be multispectral with tens of relatively coarse bands (e.g., 50- to 100-nm wide) spread over the visible to near-infrared (NIR) to short-wave infrared (SWIR) spectral range with spatial resolutions that, depending on the basing, can be very high (inches to feet) to coarse (meters). These sensing concepts will be used predominately in the daytime. The technology to achieve such capability is off-the-shelf and will even be available in commercial applications.

For example, Landsat and Systeme Probatoire d'Observation de la Terre (SPOT) satellite multispectral imagery in the visible through NIR portion of the spectrum has been used for terrain classification, trafficability assessment, and change detection as well as commercial applications in agriculture, geology, and resource monitoring. There is even promising work by some groups in detecting military targets that are significantly underresolved (say 5 percent pixel fill) in Landsat imagery. The U.S. Air Force has successfully demonstrated reliable automatic target detection in airborne multispectral imagery in the visible through SWIR region. The Navy and Marine Corps have also demonstrated reliable detection of surface minefields from the Pioneer UAV using six bands in the visible region.

Most airborne spectral imagers are multispectral with 5 to 20 bands spanning the visible to SWIR region. Some systems are confined to wavelengths shorter that the cutoff wavelength of silicon detectors at about 1 micron. Typical spectral

bandwidth is about 100 nm. Typical instantaneous field of view (IFOV) is about 1 mrad, giving ground resolutions ranging from a few centimeters from low-altitude UAVs to 20 m from U-2 altitudes. In many cases these sensors have been developed more for commercial mapping applications than for military applications and can be expected to be available at decreasing cost as time progresses.

A natural evolution of the sensing concepts outlined above would be to operate in the same spectral regions but measure many (say hundreds) of narrow (10 nm or so) bands. This hyperspectral measurement approach is enabled by the advances in large focal plane array (FPA) technology and can support the sensing of very narrow spectral features for specific target discrimination tasks or to enable adaptive measurement of fewer or coarser bands (through postdetection aggregation) depending on the application or mission of interest. At present, very compact and efficient instruments can be built in the visible spectral range; complexity grows as multiple FPAs are needed to span a broader spectral range.

Hyperspectral sensors are currently being developed primarily for research into military applications. One well-known experimental sensor is HYDICE, which has 210 bands from 0.4 to 2.5 microns with a 0.5-mrad IFOV. Flown in a Convair CV-580, it achieves 1-m resolution on the ground. Hyperspectral imaging is usually obtained by using a slit and a prism or grating spectrometer. This instrument produces a two-dimensional image with one dimension of space and the other dimension of wavelength. The true image is built up by "pushbrooming" the sensor with aircraft motion. The number of spatial samples and wavelength bands is determined by the size of the focal plane array. Silicon arrays for visible and NIR sensing can easily be in the $1{,}000 \times 1{,}000$ size. Another example, the Navy PHILLS sensor, uses a silicon CCD detector and has about 400 bands in this region. The spectral bandwidths of this system are even smaller than 10 nm. In the SWIR, a different detector material must be used. Indium antimonide (InSb) is often the choice (as was true with HYDICE). InSb arrays are limited to about 512×512 in size. One can expect further increases in size and decreases in cost. The signal-to-noise ratio (SNR) of current systems ranges from 50 to 200. It is limited primarily by detector noise, which perhaps will improve with further research in InSb and other detector materials.

Processing of hyperspectral imagery is still in its infancy. If a sensor is well calibrated (and few are), the spectral signature from a pixel containing only one type of material may be fairly easily matched to a (laboratory) reference spectrum. However, in actual images, few pixels contain just one type of material. In this case, spectral unmixing methods must be used. The pure signatures to be found in a scene must be determined (sometimes from examination of the scene to identify pure or "basis" spectra) and used to estimate the proportions of different materials to be found in any one pixel. It is computationally difficult to determine these pure signatures in a hyperspectral space of typically 100 to 200 dimensions. The problem is complicated by the fact that scene composition and therefore the "basis" spectra change from place to place in the scene. It is

expected that considerable improvement in this process will come from further work and experience with hyperspectral data.

A second important growth path is to exploit the spectral character of clutter and manmade objects in the mid- and long-wave IR spectral regime. Recently, the Air Force and Navy have shown through single pixel Fourier transform spectrometer measurements that military targets (including CCD) have good color contrast with the background. This contrast is often 1 to 2 percent of the total available signal. The measurements have also shown that for individual narrow bands, significant band-to-band correlation exists between both midwave and long-wave subbands and that the background correlation is quite high (typically 0.999 to 0.99999). This implies that background variations due to temperature variations (which are typically 5 to 10 percent of the scene signal) can be estimated in one band and used to cancel clutter in the other band. A two-band spectral sensor on the long-wave IR can often achieve an "effective" signal-to-clutter ratio (SCR) of 10 to 20 when an otherwise equivalent single-band sensor would have an SCR of less than 1. To exploit this correlation structure, it is necessary of course to have an extremely low noise sensor; i.e., an SNR of 1,000 or greater is required. Fortunately in many applications there is sufficient signal so that such SNR levels can be achieved in a relatively short time by multiframe integration. This area will also benefit from improved detector arrays that are spatially registered, like the quantum-well devices.

In summary, this phenomenon can be used to separate the effects of temperature and material emissivity as viewed through apparent irradiance as well as to compensate for the effects of the intervening atmosphere. With proper sensor design (significant signal-to-noise ratios), the sensor can be operated (with post-detection processing) as though it is noise-limited as opposed to the more common clutter-limited operation. This shows great promise for detection and classification of deeply hidden targets and can support nighttime operation.

Active Multispectral Imaging

While passive multispectral methods have been developed and utilized for many years, it follows that there is an active system analog that has not received significant attention, but is likely to play an important role in future systems. Rather than using solar or thermal (passive) spectral signatures, the active version will make use of lasers for illuminating scenes at specific wavelengths to interrogate their reflective spectral features. The primary driver for using active multispectral sensing is that, unlike passive sensors, the illumination and apparent reflectivities are not dependent on sun illumination and are not dependent on the thermal status of the target. Thus a great deal of the variability of the spectral signature can be controlled by the active illuminator. This benefit comes with certain limitations, however. In particular, active systems are limited in their ability to perform wide-area search because of the limited available laser power

levels. With the development of high-power, robust, wavelength-agile lasers, active multispectral imaging does show promise for many applications.

One possible scenario envisioned for active multispectral sensors is the assessment of littoral regions. An aircraft containing an active multispectral sensor could fly along the coast with the laser scanning perpendicularly to the flight path to form a swath image of the littoral region. The platform altitude and swath width would be limited by laser power. This system could provide both daytime and nighttime operation. Laser wavelengths that cannot be detected with the naked eye or with standard night vision instruments could be used. The laser could be range-gated to avoid bias from backscatter from aerosols and fog, and, using blue-green wavelengths, could also image under the water to assess depth and look for underwater mines. The envisioned active sensor would scan the ground with a beam composed of light from a set of lasers. The specific wavelengths would be tuned to detect targets of interest via their spectral features. For example, to detect land mines, one could look for specific features of the paint by tuning the lasers to known wavelengths where the specific paint exhibits high contrast. Also, one could look for specific types of camouflage, vehicle paint, or disturbed soil.

For missions evaluated thus far, active systems inherently require fewer bands than passive systems because the signatures have less variability due to time-varying signature properties such as sun-illumination, or cloud cover. Many missions require as few as two or three wavelengths.

Active multispectral methods could also be used for long-distance target identification. Once a target is detected by radar, a multispectral laser sensor could be used to interrogate the target of interest. Again, a range-gated laser system would be used to avoid the difficulties of atmospheric scattering and path irradiance encountered with passive systems. The spectral distribution of the illuminating lasers could be tuned to interrogate a specific target class to perform long-range identification.

One final application for laser systems is the detection and identification of "soft" targets such as gas clouds that may contain chemical or biological warfare agents, or missile or aircraft plumes. The spectral features of these targets are, again, interrogated with a set of specific laser wavelengths. The returns are thus available to conduct detection and identification. Both color signature and differential absorption techniques could be used to perform identification of cloud or plume contents, but could also evaluate plumes via their shapes or dispersal patterns.

Finally, active multispectral measurements can be coupled with additional laser discriminants to perform more thorough target identification. Active systems can readily measure a target's range and three-dimensional shape via pulsed illumination. Also by illuminating with polarized light and having two polarization detection channels, one can measure the amount of depolarization from a

target. It has been shown that manmade objects retain polarization, whereas natural targets tend to depolarize the return.

In summary, active imaging systems show promise for providing additional discriminants that can be used to detect and identify manmade targets that are deeply hidden. The discriminants available from active systems include spectral response, polarization, and three-dimensional spatial shape.

Electronic Beam Steering

Optical sensors are currently burdened with heavy, complex, and expensive gimbals. Electronic optical-phased array technology has the potential to provide lightweight, agile, and simple beam-steering subsystems that not only can rapidly and accurately point a single beam but also can point multiple simultaneous beams. Electronic steering of optical beams can be divided into two areas. One is the steering of narrowband (nearly monochromatic) light, such as with laser-based systems, and the other is the steering of wideband light as used in passive systems. Steering of monochromatic light is technologically easier since chromatic dispersive devices can be used directly and true time delay techniques are not required. It may be possible to design compact compensating optics that will allow useful wideband beam steering with intrinsically dispersive devices.

The use of a spatial light modulator as a grating with an electronically controllable spatial frequency can be used as an optical phased-array modulator (OPAM) for steering in either a transmitting or receiving mode. OPAMs can operate as amplitude or phase devices, with continuous or binary levels of control, and in pixel or continuous spatial formats. The most efficient OPAM would be a pure phase modulator with multiple phase levels. Such initial OPAMs have been constructed with two technologies that appear attractive for fabricating high-capability devices in the future. These devices use either electronically controlled liquid crystals or quantum-well Fabry-Perot vertical cavities to generate the phase shifts. Liquid-crystal OPAMs with apertures on the order of 4 cm $\times$ 4 cm have been fabricated for steering green, red, and 1.06-micrometer wavelength light. Using these liquid-crystal devices, steering efficiencies of 57 percent over 4 degrees of scan have been achieved with switching times on the order of a few milliseconds. Switching times on the order of tens of microseconds seem possible with such devices. More recently, quantum-well devices have been constructed showing 3 degrees of switching capability over a small area at 830 nanometers. These devices have the potential of switching times in the tens of nanoseconds with operation over much larger angles and sizes. Both technologies allow scaling to larger devices and mass production to reduce the device costs.

Continued progress in the development of coherent surface-emitting laser diode arrays may allow useful direct laser beam steering. Electronically steerable

narrow-beamwidth light has been generated using two-dimensional grating-surface-emitting diode laser arrays.

Video and Related Imaging Technologies

A revolution is under way in the commercial video area that will develop very high frame rate, high-pixel/resolution formats, high dynamic range (12 bits), and electronically stabilized imagery. For example, formats with pixel-sizes of 1,000 by 1,000 running at 500 to 1,000 frames per second seem possible. (At sizes of 5,000 ×5,000 pixels, the rates will be a few frames per second.) These megapixel cameras will have a great impact on our ability to do the ISR and targeting missions. Moreover, they will enable either synoptic-area surveillance (using advanced mosaic technologies under development) or spot sensors to provide either high-resolution or moving target imagery. Because of the high frame rate, video sensors are invaluable for detection of real-time change and motion.

Another certain growth path is the expansion of video technology into the infrared to enable nighttime operation. Initially these cameras will be cooled, have formats in the 500 ×500 pixel class and operate at 30 frames per second. Eventually a 1,000 ×1,000 pixel system operating at 500 frames per second seems possible. The systems will operate at room temperature and will becoming increasingly affordable as commercial applications expand.

Long-range Laser Designation

Military missions of the future will employ long-range laser designators to reduce U.S. casualties and increase weapon effectiveness. The system could include UAV or satellite-based laser designators. These designators will receive target coordinate information from other off-board sensors and then be directed to maintain a laser spot on the target for the duration of the laser-guided munition flyout. These munitions are delivered by either artillery or fighter aircraft. A significant feature of a designator system is that it does not rely on the pilot and his platform to perform target identification, designation, or bomb damage assessment. The pilot flies near the target, releases the weapon, and then leaves the area, thus minimizing the risk of being hit by enemy fire.

Another advantage of long-range designation is that in times of military conflict, high-altitude targets would likely be equipped with GPS jamming equipment. This would make GPS-guided munitions less effective. A laser designation system, in contrast, would not be susceptible to GPS jamming. In contrast, this laser system is limited by the requirement for a clear line of sight (no clouds) to the target.

There are two possible modes of operation for a long-range designation system: one in which the designating platform does not receive energy from the designating beam (open loop) and one in which the designating platform receives

and uses energy from the laser spot to derive pointing information (closed loop). The first system type would use a star tracker to determine its orientation and precision GPS to determine its location. Target coordinates would be delivered to the platform. The designator would then illuminate the target for the period from weapon release to impact. The designating platform might contain an imaging system to perform some functions; however, laser radiation would not be used to close the loop with the designator. The advantage of this system is that the laser power does not have to be boosted to compensate for the $1/(R^2)$ loss on the return path to the designator. As a result, the laser power requirements would roughly match current laser power levels. This is attractive because low laser power allows the designator platform to be less complex (due to smaller aperture sizes, a smaller laser, and relaxed cooling requirement) and less observable. The technical question remaining is the degree to which an illuminating beam can be maintained on target in the presence of turbulence and scintillation.

In order to ensure that turbulence effects are properly compensated for, a closed-loop alternative in which the designating platform uses energy from the designating beam to derive beam pointing information, is one where the beam power must be significantly larger to ensure suitable contrast for the in-band laser tracking loop. Depending on the required standoff range, this requires a significantly more powerful laser.

One auxiliary use of long-range designators would be to activate laser defenses (smoke bombs) that protect targets. Triggering of smoke-bomb defenses would confuse the enemy and make the target location more obvious for subsequent missions.

Polarimetric Infrared Imaging

Polarization is an additional element of measurement diversity that can be exploited to improve clutter suppression, target discrimination, and object characterization. Measurement experience supports the general statement that the emitted signature of manmade objects tends to be partially polarized, while natural clutter (including ocean and terrestrial backgrounds) is highly correlated among the linear Stokes vector elements. Thus this measurement scheme, coupled with suitable processing, leads to the capability to detect very low contrast (dim) targets in cluttered scenes that are not observable (without target motion) using traditional radiometric imaging. Polarimetry also offers an ability to perform emissivity/temperature separation and, since the orientation of linear polarization radiance vectors is determined by the emitting surface normal, target geometry estimation.

Exploiting polarization for clutter suppression is challenging because Stokes vector measurements must be made with excellent spatial and temporal registration, sensitivity, and relative calibration between channels. Typically, channel pixel alignments to 1 percent or better and sensitivities/relative calibration errors

on the order of 10 mK are required. Current technology uses modest-sized FPAs (128×128) with deep wells (10 to 30×10^6) and discrete component optical systems to achieve this performance. Future technology will allow denser FPA implementations with the necessary sensitivity (using analog or integrated digital technology) along with integrated optical components (to maintain precision alignment tolerances) and mixed measurements with other diversity options (e.g., color or phase).

Improved Focal Plane Array Technologies

Focal plane array developments over the next 35 years will be determined by a combination of supply-and-demand forces—the demand forces of the commercial and military marketplace and the supply forces that are "fueled" by related technology developments in university and corporate research laboratories. The panel first considered the FPA developments that are likely due to the forces of market demand and next considered some of the emerging areas of technology development that are likely to occur due to related research and development.

Commercial and Other Nonmilitary Market Demand Forces

The demand forces of the commercial and nonmilitary marketplace will be responsible for technology improvements that will directly benefit military applications of focal plane arrays. These market areas include:

- Facility or site surveillance (for security needs, law enforcement, drug interdiction);
- Remote sensing (meteorological needs, land use, geological exploration);
- Industrial inspection;
- Entertainment industry—high-definition television (HDTV);
- Automotive industry (augmented low-light-level and night vision); and
- Astronomy and scientific research.

General areas where improvements in FPA technology can be expected to develop include:

- Larger number of pixels per array;
- Smaller interpixel spacing (detector element pitch);
- Increased reliability;
- Improved producibility (with lower cost);
- Better sensitivity, lower noise, better uniformity;
- Room temperature/uncooled IR FPAs (e.g., micro-bolometer array); and
- Faster frame/readout rates.

As noted above, the move to HDTV standards will result in inexpensive (megapixel) arrays in the 2,000 × 2,000 class. Frame rates in excess of 60 Hz, for example, more like 1,000 Hz, will be commonplace. At a slower rate, digital photography markets will demand arrays in the 20,000 × 20,000 class to satisfy professional requirements. Smaller interpixel spacing will result from the commercial demand to have even smaller optical camera systems.

Currently, the cryo-cooler accounts for about 90 percent of the cost of an IR detector assembly. Thus only those applications that require high performance (noise equivalent detection temperature [NEDT] much less than 0.1 K) will utilize cooled IR. Driven by the need for private surveillance, law enforcement, and night vision for motorists, there will be uncooled arrays that support 0.1-K NEDT sensitivity.

The current limitation for hybrid mercury-cadmium-telluride (HgCdTe) arrays due to thermal mismatch will be overcome by using new lithographic techniques now under development. Array sizes in the 1,000 × 1,000 class seem feasible in the near term.

Developments in market areas related to digital imaging technology can also be expected to indirectly assist the development of focal plane array technology. These areas include the following:

- Digital image compression, storage, and transmission; and
- Digital image manipulation and display.

These FPA and FPA-related developments in the commercial marketplace can be expected to keep pace with the general needs of the Navy in the areas of communications, operations, and some space-based needs (e.g., meteorological).

Military Market Demand Forces

Military application areas with a continuing strong Navy need that is not likely to be met by developments in the commercial marketplace are as follows:

- Missile warning receivers;
- Bomb, missile, and projectile guidance; and
- Identification friend or foe.

The above applications are less affected by developments in the commercial sector since information processing techniques required to discriminate targets from background clutter and perform target identification must exploit unique signatures of the target and background. These unique characteristics include spatial and temporal features as well as electromagnetic wavelength and polarization. As discussed above, the sensing of these unique radiation characteristics requires the use of specialized detectors (and optical methods) to achieve target

signal-to-background-clutter ratios adequate to provide acceptable detection (or discrimination) and false alarm probabilities.

In the above application areas, the demand will be for multiband focal plane arrays (for spectral discrimination) with a large number of elements (for wide field-of-view coverage) and dense detector elements (for compact and lightweight systems). Since the wavelength bands most suited for a particular target and background vary greatly, a means to "tune" the spectral bandpasses is necessary. Detection techniques (perhaps using quantum wells) that can be spectrally configured in real time will permit the fielding of sensors that are "agile"—more adaptive to terrain and target variations and more general purpose.

Due to the unique FPA architectures that must be developed and the lessor need in the commercial marketplace for such capabilities, continued FPA development in the above application areas will require government funding.

Research and Development Impacts on FPA Technology

Many incremental improvements in FPA technology will naturally occur due to the commercial and military market forces discussed above. Research and development efforts in university, corporate, and government laboratories will result in likely breakthroughs in areas related to FPA technology:

- Development of synthetic materials (e.g., nano-technology); and
- The understanding and emulation of biological systems, particularly in the areas of visual processing methods.

Progress in these areas is more difficult to predict, but can be expected to result in the following:

- Detector materials whose detection properties can be controlled in real time;
- On-chip (or close proximity) parallel processing for temporal change (e.g., motion); and
- Processing characteristics that can be configured (in near real time) for a particular mission, i.e., provide a multirole sensor.

Progress in research and development efforts that can be expected to substantially improve FPA technology will depend strongly on government basic and applied research funding levels.

Phase/Wavelength Diversity for Aperture Synthesis

Optical aberrations that degrade image quality and resolution can arise from atmospheric turbulence, mirror misfigure, and misalignments among optical com-

ponents. A variety of sophisticated techniques have been developed to combat the effects of such aberrations. One of the most compelling of these is a technique known as phase diversity. A phase-diversity data set consists of two images. The first is a conventional focal-plane image that has been degraded by the unknown aberrations. A second image of the same object is formed by perturbing these unknown aberrations in some known fashion, thus creating phase diversity, and the reimaging. This can be accomplished with very simple optical hardware. For example, the combination of a simple beam splitter and a second detector array, translated along the optical axis, further degrades the imagery with a known amount of defocus. Alternatively, both images can be simultaneously collected on the same camera with the use of a prism. Notice that the second image will be degraded by the original aberrations in addition to the known defocus. It is rather remarkable that these two images can be digitally processed to "jointly" estimate both the unknown aberrations and the undegraded image that would have formed in the absence of any aberrations.

Phase diversity has been used to retrieve diffraction-limited images of solar granulation using ground-based telescope data, thus overcoming the degrading effects of daytime atmospheric turbulence. In solar astronomy, phase diversity is making the transition from academic curiosity to routine operation. Phase diversity has also been successfully demonstrated in nighttime astronomy. Some of the most impressive reconstructions to date have come from applying phase-diversity methods to ground-based images of satellites where adaptive-optics correction was used. In this case, phase diversity was used to overcome residual aberrations not compensated for by the adaptive optics. The resulting improvement in image quality and resolution is dramatic.

Technology Trends for Phase Diversity

Several alternative solutions to the problem of imaging in the presence of aberrations require expensive and complicated hardware, including Shack-Hartmann wavefront sensors and/or deformable mirrors. By contrast, phase-diversity technology requires only simple optical hardware at the cost of increased computational burden. In addition, the phase-diversity algorithm is evolving rapidly with respect to computational speed. Continued gains in algorithm speed can be anticipated with the integration of concepts such as improved initial estimates, tracking aberration evolution, and precomputing with neural networks. A special-purpose computing architecture using off-the-shelf components was recently designed for processing phase-diverse speckle (a variant on phase diversity) data. This special-purpose computer would produce 64×64 image reconstructions at video rates and evolving aberration estimates at an update rate of about 160 Hz. Given current trends in computing hardware and projections in algorithm development, it should be possible in a decade to process phase-diversity reconstructions of large images at kilohertz rates.

To date, phase diversity has been applied to imaging scenarios for which the aberrations are well modeled as localized to the pupil. This is a valid model for turbulence-induced aberrations in upward-looking scenarios. However, there are many applications of interest with horizontal-path or standoff geometries in which a volume turbulence model must be adopted. The volume-turbulence problem is considerably more challenging because the image blur function will change across the field of view (space variance). In addition, amplitude aberration (scintillation) is often a factor. As a consequence, there are more parameters to estimate, and the computations required are considerably more burdensome. Preliminary simulations suggest that phase diversity can be used to recover undegraded images in these challenging scenarios. However, the problem of imaging through volume-turbulence is sufficiently challenging that both pre- and postprocessing will likely be needed. It is projected that, in the next 15 years, phase-diversity technology in conjunction with adaptive optics will provide a means of collecting diffraction-limited images through volume turbulence.

A technology known as wavelength diversity, a close relative of phase diversity, was recently suggested for use in multi- and hyperspectral systems. In such systems, the performance of classification and identification tasks is enhanced when spatial resolution is improved. Therefore, the determination of aberrations in such systems can significantly improve performance. Like phase diversity, wavelength diversity affords the joint estimation of the system aberrations and the images that would have formed in the absence of any aberrations. However, wavelength diversity can be accomplished with a raw multispectral data set and does not require any system changes to obtain defocused images, because the "diversity" comes from the change in wavelength, which is already built into a multispectral data set. Wavelength diversity has been demonstrated in simulation, although the algorithms are embryonic at this stage. As exploitation of multispectral data matures so that spatial resolution becomes more important, wavelength diversity will provide increased performance at no additional sensor cost.

Future Applications

A capability for imaging through volume turbulence lends itself to a variety of uses in ship-based, littoral missions. In such scenarios, a ship-based telescope located up to tens of kilometers from the shore could recover diffraction-limited imagery while imaging through extended-path turbulence. Such imagery could be used for surveillance, targeting, and bomb damage assessment. At these ranges, the aperture can be relatively small while still acquiring very fine-resolution images. For example, if the range is 5 km, diffraction-limited resolution of 2 cm can be achieved with a telescope primary that has a diameter of about 12 cm at visible wavelengths. Given a video-rate processing capability, such assets will be particularly useful for time-critical monitoring of rapidly developing events.

A significant portion of the cost of space-based optical platforms is the cost

of launch, owing to the weight of the system. This is particularly true of long-dwell systems, but is also true for a fleet of LEO platforms. A candidate solution to the current technology shortfall is to relax optical (and structural) tolerances (thereby reducing weight) on the primary mirror(s) and recover the loss with postdetection processing via phase diversity. The driving principle is to "trade mirror mass for megaflops." This is a favorable tradeoff, given the cost/performance trends in computing technology. By allowing optical tolerances in the primary collector to be relaxed, one seeks to achieve (1) a significant reduction in structural weight, (2) simplified deployment, and (3) reduced fabrication expense. The added freedom in design afforded by relaxing optical tolerances suggests unconventional concepts for light collection. For example, the primary collector might be nonrigid (floppy), monolithic or segmented, filled or sparse. The collector could be a very thin, mylar surface stretched over a skeleton structure that could be deployed like an umbrella or could be inflated upon deployment. Time-varying aberrations that would be introduced with relaxed structural tolerances (by differential solar heating, mechanical vibrations, and so on) would then be overcome with phase-diversity methods. It may be important to design for a small compensating element conjugate to the primary collector to compensate for gross figure errors in the primary. Such compensation could be passive (fixed) or possibly active with a large dynamic range. Residual aberrations would then be overcome with postdetection processing. Note that optical precision is needed only on this small element and not on the large primary collector. Relaxed-optical-tolerance imaging concepts offer a low-cost approach to real-time, fine-resolution imaging with global coverage.

Passive Interferometric (Synthetic Aperture) Imaging

Interferometric measurements can be used in the visible or infrared region to "synthesize" an aperture in the same manner as is done in (active, coherent) SAR. Passive synthetic aperture can be constructed to defeat the diffraction limit of the collecting telescope or to provide differential range information so that a three-dimensional representation of an object can be collected.

As an example, interferometric imaging systems are being used for fine-resolution astrometry purposes. Astrometry is especially important to establish databases of star locations for star-tracking systems. These applications are effectively addressed by using multiaperture interferometric imaging systems. One such system, the naval prototype optical instruments (NPOI), is a long-baseline multiple-aperture imaging system. By using multiple apertures obtaining image information via interference phenomenon, systems such as NPOI are able to obtain fine-resolution images while avoiding the expense of large monolithic apertures.

In the future, passive interferometric systems will also be used for several other purposes. One of these is to perform passive synthetic aperture three-

dimensional imaging of military targets. With such a system, an airborne or space-based platform would be equipped with a relatively small multiple-aperture image collection system. It has been demonstrated that the relative motion between the platform and the stationary scene can be used to synthesize a (larger) imaging aperture. Two-dimensional images that are more than a factor of 10 better in resolution relative to the diffraction-limited collection aperture have been demonstrated in the visible and infrared spectral bands. Furthermore, a passive multiple-aperture system has been used to collect three-dimensional images of tactical targets at 2-km range in the mid-wave infrared (MWIR) bands. Yet another use of the passive interferometric imaging mode is to perform the radar analog of moving target detection. To accomplish this one measures the Doppler beating of light that originates from a single object point but propagates through separate apertures, or paths before interfering in the image plane. Geometrical path differences between the two optical paths cause the light to exhibit differential Doppler shifts. By examining the temporal content of the optical interferogram, one can readily measure the differences between stationary and moving targets to perform moving target identification with a passive multiple-aperture system.

In summary, interferometric optical systems show promise for passively providing additional target information based on either better-spatial-resolution, three-dimensional shape measurement, or detection of target motion through the processing of differential doppler signatures.

CONCLUSIONS

Future surveillance capabilities in support of force projection ashore will be truly astounding compared to what exists today, yet no scientific breakthroughs are necessary to achieve them. The expansion in scale of today's sensor systems in radar, electro-optics, acoustics, and SIGINT enabled by computer and communications technologies coming from the commercial sector will make it happen at an affordable price. Much thought must be given to platform issues and concepts of deployment, however, so as to understand the cost-survivability-performance tradeoffs necessary to guide future Navy investment. Since most future conflicts will be fought jointly with other components and coalition partners, every effort must be made to provide connectivity and interoperability with surveillance platforms of the other Services and of U.S. allies, taking advantage of the bandwidth revolution occurring in communications technology. The Department of the Navy should consider, however, the development of organic sensor platforms to support surveillance of the littorals during the early stages of conflict where the Navy/Marine Corps team will be first on the scene. Each sensor capability must be extrapolated in light of credible countermeasures an enemy might take to defeat its effectiveness, and in light of the estimated difficulty of achieving fully automated exploitation tools for its utilization. The ability to perform target

classification or identification based on radar sensor data alone is an area where much progress must be made. The incorporation of surveillance systems into larger architectures to perform specific military missions only emphasizes the importance of the identification problem. Although the goal of "near-perfect knowledge" may never, in fact, be truly achievable due to fundamental physical limitations, removal of implementation limitations through advanced technology will nonetheless provide surveillance systems that will be dramatic force multipliers for future naval forces.

5

Information Warfare

INTRODUCTION

Given the critical centrality of information to every aspect of naval operations, the area of information operations (IO) and information warfare (IW) assumes a critical posture. The Department of the Navy must assure the availability and integrity of the information infrastructure and information content on which it relies, and must create and maintain required confidentiality. In an era of prolific information gatherers and promulgators as described in Chapters 2 through 4, these attributes must apply not only to the information systems but also to the operational posture of the fleet. The treatment of active and passive hiding measures, which in the past have been dealt with by radio silence or other means, is becoming an integrated part of the whole IW operational posture. The tactics to minimize observables not only will include decisions to radiate or not, in the conventional sense, but also must include the entire information set in every dimension and through every medium, including the ether, space, air, undersea, and cyberspace.

While minimizing its own information vulnerability, the Navy Department will need to defend its information infrastructure and information content against attack, using both passive and active means. These means must include comprehensive information security practices as well as technologies that assist in detecting and eradicating attacks. The most primitive of these types of technologies are virus checkers, automated audit analysis programs, and those based on zener diodes. With the increasing importance of these types of technologies and applications, it is critical that the Navy Department stay abreast of related developments in the commercial sector.

While denying the adversary information, the Department of the Navy may also need to employ active measures to manipulate, corrupt, or destroy information as necessary. Use of methods such as jamming, deception, and psychological operations can be continued and extended through capabilities provided by rapid growth worldwide of information technologies for activities such as network-based operations.

These requirements are complicated by the Navy's increasing dependence on, and interconnectivity with, public and commercial information sources and infrastructure elements. The commercial aspects of the Navy Department's information environment must not prevent its effective exploitation and protection of the information infrastructure or content. The associated challenges must be aggressively recognized, analyzed, and acted upon.

This chapter discusses the technical areas that support the development of an effective capability to conduct information operations and warfare in the time frame of 2035. While the discussion focuses on specific technologies, the crucial importance of people and organizations, particularly in creating and maintaining a robust defensive posture, must not be overlooked. In particular, the panel argues that the Department of the Navy should:

- Continue to exercise the full spectrum of IW in an effort to establish policy and procedures in preparation for hostilities or conflict such that it involves all levels of government-military leadership;
- Continue to make IW activities operational, integrating defensive and offensive elements at the control of the warfighter and developing a clear operational vision of what really can and what really cannot (or will not) be accomplished with IW; and
- Invest in specific technology applications, including those that can support countermeasures and defensive capabilities, offensive capabilities, and intelligence support activities, as detailed in this chapter.

INFORMATION WARFARE IN A GLOBAL INFORMATION ENVIRONMENT

Because of the fundamental changes in the worldwide information environment described in this study, it is crucial that the warfighter have a clear vision of what he can and cannot do in the information dimension in terms of warfare activities. The ownership of infrastructure elements and information content is a significant issue to be considered. There has been considerable hand waving about attacking an adversary's information and/or supporting infrastructure in order to deny him the use and leveraging capabilities of information, but the lessons learned from a number of military exercises seem to indicate that to date little well-thought-out policy or practice has been developed. There are three issues here:

1. Information and information infrastructure likely will not be wholly owned, operated, maintained, or protected by the adversary in any great part—just as the U.S. Department of the Navy will be using commercially provided data over commercially provided and maintained infrastructure elements, so also will the adversary. Those portions of the infrastructure may be "off limits" to attack due to some combination of commercial, international, or social concerns.

2. The application of acts of war to the parts of the adversary's information infrastructure that are fair game likely will be denied to the warfighter until after hostilities are engaged in.

3. The effective demonstration of the full range of IW capabilities will involve many or all government organizations, which will establish critical vulnerabilities, policies, and procedures.

Given these constraints, there are clearly things that the Department of the Navy must have the ability to do. First, the warfighter must have the ability to defend his information content and infrastructure against attack, destruction, or degradation. Defensive information warfare has three elements:

- *Protection against hostile activity or attacks*. Protection includes developing and applying technological and/or procedural fixes to vulnerabilities, creating and enforcing information policies and management standards, applying reasonable personnel security policies (such as background checks, two-person software upgrade control procedures, and restrictions on possible actions), and protecting the physical environment of critical resources (through the use of gates, guards, locks, and emergency support facilities), as well as continually reassessing risk.
- *Detection of hostile activities*. Detection includes such activities as monitoring the operating environment, auditing accesses and usage patterns on systems, performing periodic reassessments of personnel and physical facilities, and checking the integrity of software and data.
- *Reaction and correction*. Reacting to an attack or a problem includes correcting what has been done if possible, conducting triage on the system if necessary (including turning off elements of the system and rerouting network connections), increasing protective elements, and reconstituting capabilities, as well as potentially moving operations to a backup or alternate facility or subinfrastructure.

The elements of defense include much more than just technologies and apply to both the information content and infrastructure. Managing information vulnerability is enabled by these activities.

It is conceivable that in the future information environment there will be a requirement for the warfighter to be able to change his defensive posture in response to changing environments, such as mission requirements, or in order to

be able to interoperate with an ally—and to immediately cease that interoperability on demand. The warfighter, therefore, must be in control of his defensive capabilities and be able to employ tactics and techniques to minimize or mitigate the effects of hostile activities.

The tools at hand to do this must include both technologies and procedures. Of the technologies, some percentage will be commercially produced—including, potentially, encryption products. The key to a robust and resilient defense is the knowledgeable application and management of the defensive components: the warfighter must be in charge of this process, must feel responsible for the results, and must have the appropriate capabilities and personnel to support the defensive posture.

Second, the warfighter must have the ability to attack and deny the enemy the advantage of those elements of the adversary's information content and infrastructure that are fair game. Even considering the element of accidental resiliency that may exist due to multiple paths and sources, it must not be forgotten or overlooked that there can be real utility in attacking certain targets. For example, denying a specific air defense system may not prevent indication and warning, since the data supporting that function could come in via the Cable News Network (CNN) or on e-mail. But denying that air defense system would limit a real-time link between the indication and warning function and a weapons system, thus injecting a time delay into the adversary's observe, orient, decide, and act (OODA) loop.

The warfighter must understand what these targets are, how to attack them, how to integrate these attacks into the operations priorities, and how to measure the contribution to mission objectives. These requirements speak to a robust supporting structure of exercises, training, assessments, and intelligence.

TECHNOLOGY THRUST AREAS

Technologies for IW Defense

Countermeasure and defensive efforts to date have been focused on patchwork approaches to security. To ensure the secrecy and integrity of data during transmission, cryptography has been used. To limit access, mechanisms have been employed that require varying degrees of identification and authentication. To ensure integrity in storage, cyclic redundancy checks and other techniques have been employed. To ensure availability, multiple copies have been transmitted and backups made. A significant infrastructure has developed to coordinate and manage the use of these techniques and technologies.

Developing defenses implies knowing not only what one's own vulnerabilities and susceptibilities are but also what is required to mount an attack on one's systems, as well as what the logical outcomes might be. This is a fundamental part of risk management. The marshaling of resources and knowledge to attack

one target implies a baseline of complexity, but the addition of each new target makes the proposition exponentially more difficult. Further, if the targeting has the intention of preventing reconstitution of capability, then secondary targets must also be attacked. In addition to the direct resources involved, conducting such an operation requires a very large amount of intelligence information: where the critical vulnerabilities are, how they can be attacked, and how the attacks will be coordinated are merely the most obvious questions. Additional information of value to the attackers includes an understanding of the timing required for successful attacks, what actions would be required to prevent immediate reconstitution of the target, and the ability to predict effects with some degree of certainty. These are nontrivial requirements.

The technologies contributing to IW defense are aimed at providing confidentiality, maintaining integrity, and ensuring availability. These capabilities are currently provided in high-assurance environments, depending on the type of information to be protected, and there has been little attention to date to how to provide these capabilities in low-assurance environments. The envisioned future world of systems of systems created freely out of COTS products linked together in fluid and unmanaged networks stipulates an increased emphasis on how to provide enough confidentiality, integrity, and availability in a low-assurance environment.

Clearly, the use of cryptography bears a great deal of application in such a world. Besides protecting data at rest and in transit, crytography can enable localized strong identification and authentication (I&A) of both human users and software objects. It can also enable applications such as "tunneling" creating cryptographically protected virtual private networks (VPNs) embedded in unencrypted networks, and packet-level integrity maintenance, including both integrity verification and tamper checking, beyond what is currently provided for in communications protocols. Research in these areas could potentially provide the critical technologies needed for robust and resilient information transfer in a hostile world infosphere. Cryptography is not the sole key to these problems, however. Research in software engineering and computer hardware engineering is required in order to develop understanding of how software can be verified, how systems can be maintained in a system-of-systems environment, and how operational security can be ensured.

The U.S. security community has developed significant capabilities in protecting systems and information to date. A next step is to integrate these capabilities into a warfighting resource and develop the capabilities to control them as an integrated whole, managing them in concert with offensive efforts and operational environments as required. A candidate list of specific technology thrust areas is discussed below.

Protection and Detection

Clearly a high priority is protecting information content and infrastructure elements and detecting hostile activities. Three types of capability would provide great benefit to the warfighter:

- An automated defensive posture assessment capability,
- Truth-verification capabilities, and
- Attack-detection capabilities.

Defensive Posture Assessments

The capability to assess the defensive posture of information resources at any given time is currently a distressingly manual procedure. Even with automated data reduction techniques, the integration of the analyses is convoluted and manual, if possible at all. In order for the warfighter to understand the defensive posture of the information resources supporting and enabling the warfighting capability, it is desirable that the information environment be readily analyzable using trusted automated processes. This capability would require integrating the outputs of all auditing processes, intrusion-detection processes, risk analysis tools, and other capabilities as they are developed.

Assessment of defensive posture is critical to developing a further ability to manage information vulnerability, and it would conceptually provide the operator with the ability to minimize, obscure, or manipulate what his detected information vulnerability appears to be.

A capability to work toward would be to have a workstation (virtual or otherwise—it may be that the most useful way to interface with this data would be through a virtual reality interface) that would allow real-time assessment of the defensive posture with command and control over the elements of that posture, allowing the warfighter to modify the defensive posture in real time in response to changing conditions and environments.

Truth Verification

As dependence on information increases due to the automation of more and more elements in the surrounding environment, the ability of the warfighter to judge the reliability and accuracy of information content becomes more important. There are two aspects to this challenge:

- Judging relative truth: being able to comprehend the inherent inaccuracies in data that exist due to model uncertainty, source inaccuracies, and so on; and
- Judging continued truth: being able to determine whether the information being considered has been tampered with, replaced, or otherwise interfered with.

The significant technical challenges in both of these aspects range from human interface issues to confidentiality measures. In responding to these challenges, complex information display techniques, such as virtual reality applications, will clearly have some level of payoff. As capabilities for injecting falsehoods into otherwise truthful data continue to be developed,[1] the challenge of determining continued truthfulness will be exponentially greater, particularly in light of the automated fusion capabilities that are being relied on to assist humans in handling the huge amounts of available data in a timely manner.

Attack Detection

Being able to detect when information attacks (in any form) occur is clearly a high priority. Current-generation tools such as the Automated System Intrusion Monitor (ASIM) represent a first step in developing a real-time ability to detect such attacks. Current 6.1-level research ranging from exploration of the application of artificial intelligence to this problem[2] to an attempt to model a detection system on the human immune system[3] is laying the groundwork for developing the scientific principles that will lead to operationally useful automated intrusion detection and reaction. This nascent capability needs to be nurtured and pushed to a real-time capability for the warfighter.

React and Correct by Performing Defense Posture Realignments, Including Triage

A capability for reacting when hostile activities or accidents occur is also critical, as is the ability to correct the situation. Significant capabilities already developed relate to reconstituting and recovering information. Another primary capability that is critical to the warfighter, but that may be less important to other entities and thus not likely to receive an equitable amount of technology investment, is the capability to perform real-time defensive posture realignments, including triage of both information infrastructure and content as necessary (analogous to cutting off a finger in order to save an arm).

---

[1] Kaplan, Karen. 1997. "The Cutting Edge: 3-D Technology Blends Fact and Fantasy," *Los Angeles Times*, March 3, 1997, Home Edition, Business Section, p. 1.

[2] National Institute of Standards and Technology and National Computer Security Center. 1994. *Proceedings of the 17th National Computer Security Conference*, Baltimore, Maryland, October 11-14, 1994, National Institute of Standards and Technology, Gaithersburg, Md.

[3] D'haeseleer, P., S. Forrest, and P. Helman. 1996. "An Immunological Approach to Change Detection: Algorithms, Analysis and Implications," in *Proceedings of the 1996 IEEE Symposium on Security and Privacy*, sponsored by the IEEE Computer Society Technical Committee on Security and Privacy and the International Association of Cryptologic Research (IACR), on May 6-8, 1996, at Oakland, Calif., IEEE Computer Society Press, Los Alamitos, Calif., pp. 110-119.

For example, a warfighter performing a humanitarian relief mission in an assessed low-threat area should be able to minimize his defensive posture so as to increase his ability to perform information aspects of the mission (perhaps information dissemination operations), or if the situation becomes more hostile or threatening, to ratchet up his defensive posture accordingly. The infrastructure required to do this does not exist today. The capability for real-time assessment of the threat environment in the information dimension does not exist for the most part, nor does an ability to take such inputs and feed them back into the operational environment as part of a dynamic threat posture. A logical extension of such a capability would be the ability to determine threat and attack vectors, disconnecting systems as needed in order to channel attacks in one direction or to rebuff them completely.

Offensive Technologies

A list of technologies for offensive information warfare is easy to imagine; integration of these technologies into a time-phased operational process will be difficult. The infrastructure and the content are jointly and separately the weapons and the targets; the integration into operations provides a useful offensive capability.

Consideration of offensive IW as the application of techniques and weapons on a useful scale (where useful is relative to the results desired) against information assets and systems, when desired and with predictable results, gives a framework for dissecting what it takes to perform offensive IW operations. On the cyberspace battlefield, conducting IW requires being able to do what is needed when it is needed. A lesser capability is neither effective on a strategic level nor conducive to success in warfare.

The offensive IW community must develop techniques, tactics, and weapons to support organized and prioritized mission objectives. These could take the form of:

- Single weapons with specific goals,
- Multipurpose weapons with generic goals, or
- Attack procedures that target elements selectively in order to achieve desired results.

A subversive attack would be multidimensional—an attack that combined attacks against the various elements of the information infrastructure, such as telecommunications providers, the power grid, the logistics information network, and the news media. A coordinated attack against these entities could conceivably cause widespread disruption of service, unstable support systems, public infrastructure breakdown (such as disruption of subway systems), and rampant gossip and innuendo. To be successful, such an attack would have to disable

these elements within a short period of time (such as a few months) so as to prevent recovery within the existing governance construct. With disablement spread out over a longer period of time, patches and jury-rigging of systems could prevent the scale of result desired.

The most subversive type of strategic attack on information would incorporate deception, perhaps using IW and non-IW components, prior to the actual attack to distract the target from being able to, first, recognize the attack when it gets under way and, second, respond effectively.

The most effective way to launch an attack of strategic significance would be to combine a series of IW kinds of attacks with other non-IW types of attacks. This approach would prove most serious to an adversary's capabilities for response, in that it would tax all resources for which, potentially, no overarching coordinating function would in place.

Information Infrastructure Weapons

Clearly, a significant capability for attacking and disabling elements of the information infrastructure exists today in the form of bombs and jammers. Potentially useful technological thrust areas include weapons for nonpersistent network interruption, which in theory would allow the United States the ability to deny an adversary the use of parts or all of a network without physically damaging it, and for a controllable period of time.

Information Content Weapons

Information content weapons are those designed to go after information itself at its source, while it is in transit, or while it is being processed or displayed. The outcomes could include delay, modification, deletion of, or addition to the information.

Intelligence Support Technologies

Intelligence information is the key to developing and implementing effective information warfare plans and operations. Whether the goal is developing a system to degrade an adversary's warfighting capabilities or ensuring pretection for one's own military information systems, detailed technical information on the target's hardware, software, and operations is essential. The degree to which attackers are able to acquire timely, accurate, and complete information on the targeted system will determine the degree to which they can analyze exploitable vulnerabilities, and thereby design efficient and effective weapons and delivery vehicles, and develop useful measures of the effectiveness of their approach. The challenges inherent in the intelligence support role are underscored by the lack of a definitive national intelligence estimate on the information warfare threat:

assessing the IW threat is different from hunting for missiles and requires new sources and methods of data collection and analysis in order to support definitive intelligence conclusions. Candidate intelligence support capabilities that should be pursued include enemy profiling and targeting.

Enemy Profiling

The world is changing in ways that are hard to predict. The rise of transnational organizations with multiple loyalties is one development; the availability of information technologies to every organization that exists is yet another. Given these conditions, the development of a methodology to profile enemies in terms of intent, capabilities, and organizational structure would seem to be a high-payoff endeavor that could support the development of a comprehensive information order of battle.

Targeting

The ability to launch a cyberspace attack does not necessarily require having a precise photograph of the physical location of the target, but may be much more dependent on having a network address or knowing some other technical detail. The functional and physical entities that would serve as targets for IW enable and support information processes at differing levels of abstraction. They include the public switched telephone network (PSTN), automated teller machine networks, the financial transaction network, electronic money, credit, the Global Command-and-Control System (GCCS), tactical C^3, medical and corporate networks, weather, cars, petroleum and gas transport, logistics, process controls, interfaces, transportation, the air traffic control system, the nascent intelligent vehicle highway system (IVHS), and many others. These functional entities mask an incredibly complex set of physical entities that continually evolve and change, usually transparently to everyone except the person doing the change. To complicate matters, the functional entities represent shared interests that may in addition share physical infrastructure elements with other functional entities. This introduces the phenomenon of nonlinear cascading effects, whereby an attack on one functional entity may have an impact on other functional entities or an attack on a physical infrastructure element may affect multiple functional entities; the challenge of confining damage and affect is thus magnified, but so is the ability to target systems with predictable effects.

A comprehensive capability to perform targeting in support of information operations and warfare must address these issues.

Knowing where the high payoff targets are in cyberspace is fundamental to being able to integrate time-phased priorities for attack into mission planning. Developing targeting methodologies and identification is necessary and should

be done independently of current targeting methodologies and identification procedures to avoid getting caught in inappropriate paradigms.

Support for Attack Prioritization

There is always a physical component to an IW attack or defense, even if only at the level of the electron, and consideration of the physical paths of attack and the constraints and limitations imposed by the physical components of the attack or defense is critical. At some point, to be operable, all attack plans must identify which specific components of the system—ranging from the 0s and 1s that represent the data through to and including the persons in the system—will be attacked with what weapon or weapons. A complicating factor is that many of the physical entities that underlie the intricately interconnected information infrastructure support not a single function but many functions. An attack must be designed to take this interconnectedness into account, perhaps even exploiting this feature. Once targets have been identified, integrated planning can occur that prioritizes targets within the context of the overall attack plan. First steps to being able to do this are under way now; these efforts should be supported and encouraged.

Intelligence Preparation of the Battlefield

Performing intelligence preparation of the battlefield (IPB) is a time-tested procedure that must be expanded to include the battlefield's information dimension. This task is challenging, given that the information aspect of a battlefield is very different from its physical characteristics, with few geographic boundaries but multiple dimensions. Moreover, intelligence preparation is becoming increasingly necessary. Recognition of this aspect of IPB will help support the execution of integrated operations plans.

Damage Assessments and Measures of Outcome

A significant problem in information operations is how to measure success and the level of success in any operation. While admittedly a huge challenge, it is conceivable that the methodical examination of this problem may benefit other challenge areas as well, such as targeting and attack prioritization. Only when it is possible to identify predictable outcomes at the functional node level is it possible to begin to understand the potential impacts and isolate the intelligence requirements that provide support to both the offensive and defensive IW communities. This in turn feeds into understanding of what the essential elements of information are, what the requirements for damage assessment would be, what the intelligence collection requirements would be, and what it would take to be able to perform a successful attack.

Weapons Development Support

The data collected in the pursuit of targeting, attack prioritization, and development of measures of success are invaluable to the development of effective weapons. To quantify the effect of attacks on a specific information system requires complex analyses taking into account the physical and logical components of the system, the shared resources, and the vulnerabilities. Potentially, this type of analysis could provide insights into network vulnerabilities and provide valuable input for cost/benefit analysis of weapon development. The latter is important also for determining whether the likely results of an IW attack would outweigh its costs, risks, and uncertainties.

Quantifying the overall effectiveness of an IW attack is a complex task and will probably not result in unambiguous answers. For example, in a conventional weapons attack on a communications switching facility the results may be quantified in terms of degraded performance—the number of circuits still available and the period of outage or the level of noise on the remaining circuits. This type of information may be applied directly to an evaluation of military objectives such as the probability that critical telephone circuits have been eliminated. In a "soft" weapon attack on the same switching center, the results may be much more complex. Only in certain cases will the IW weapon be designed to remove the switching circuits from operation as if destroyed by a "software bomb." Some of these types of weapons will conceivably cause the system to pass corrupted or false data while apparently remaining fully operational. In these cases, depending on the nature of the corrupted data, it may not be possible to directly determine the effect of "bad" data on critical functions of the affected network. And, of course, the real issue is the net effect on the degradation of command and control, not the reduction in telephone circuits, although there may be a positive correlation between the two.

In addition to the complexities introduced by altering information content, evaluating the effectiveness of IW will also suffer from uncertainties about or gaps in technical information concerning configurations of the network. As an extreme and simplistic example of this concept, consider a foreign command-and-control network with two independent and parallel transmission systems. If only one of the transmission systems were known about by an attacker, then any attack, no matter how devastating to that particular system, would nevertheless leave the command-and-control network fully functional. It is likely that real information networks, particularly military systems because of their inherent security precautions, contain many components that perform redundant functions or are interrelated in ways that are difficult to discover. Further, there are complexities introduced by the technical knowledge of the people who use the systems and their willingness to improvise new and unforeseeable alternate capabilities. These are issues that complicate translating the likely effects of use of a

specific weapon into meaningful assessments of an attacked adversary's reduced military effectiveness.

Modeling and Simulation

It is clearly necessary to apply descriptive and quantitative formalism in an analysis of the effectiveness of IW attacks. Measures of IW effectiveness are not understood completely at this time, but it is clear that they must reflect changes in strategic or military posture or capabilities relative to specific attacks and defenses. The methods applied must characterize the level of confidence in the information pertaining to the targeted information system and must reflect consideration of the impacts and likelihood, where possible, of undiscovered features of the network. These undiscovered features could include redundant nodes, persons-in-the-loop, and additional functionality.

Conceptually, it is useful to divide an information system into smaller, nearly single-function modules for which it is possible to define a structure. The information system model must span both physical and functional aspects so that impacts on logical systems are described as a result of specific actions. With effective modeling and simulation comes an ability to understand targetability requirements as well as interactive effects. Further, an abstracted model can be nested, with levels of functionality abstracted within each other from the simplest to the most complex.

A model could represent an entire simple network—a small number of networked computers—or it could represent a single module in a more complex system—one air defense battery in a country's air defense network. The information input into the module could represent information input from a keyboard, data obtained from remote sensing devices (such as an early warning radar), information from other modules, or, more likely, a combination of many sources of information. The main purpose of the module would be, of course, to perform some function—send e-mail, move cargo, launch missiles, or relay refined or processed information.

With such a model it is possible to conceptualize an IW attack on any of the targetable elements of an information system: the data, the retrieval of the data from some storage medium, communication or transmission of the data, and of course the processing or manipulation of the data. Further, the impact of such an attack on the logical purposes that the physical pieces support can be described. The depth of understanding of what the model represents can be described statistically in order to characterize the degree of the certainty of that understanding. These statistical probabilities play into the equation that describes the complexity of a successful attack: at the very least, it is necessary to know how probable it is that functional relationships are operating in such a way as to be vulnerable to a particular weapon and with what probability the effect on the physical target will

track to the functional target. A next step in the abstraction is to model the weapon system.

Each target can be attacked with a weapon. Conceptually, a weapon consists of two parts: the payload for the weapon and the delivery vehicle by which the payload is transported to the target. Thus, two probabilities associated with the weapon must be considered: the probability that a delivery vehicle will successfully deliver the payload to the correct target, and the probability that the payload will successfully detonate.

The statistical modeling of impacts is a great deal more difficult. For example, how do we quantify loss of functionality when deceptive data is introduced into a system? The effects are clearly dependent on the type of system and what the purpose of the data is—in one system, the result could be an immediate loss of functionality as the processes report out of bounds outputs, whereas in another system, the result could be an insidious skewing of simulation outputs totally unnoticeable to the authorized user.

Applying such a model iteratively can enable identification of some interesting second- and third-order effects. For example, an attack scenario can be modeled and then a second attack scenario modeled over the template of the result of the first attack. This process would provide information of two general sorts: first, identifying resilient pathways and logical functions, and second, identifying second-order attack priorities. From the offensive point of view, iterative modeling is useful to refine targeting strategies; from a defensive point of view, it is invaluable in identifying strategies for triage to recover from attacks as well as identify vulnerabilities that could be made less vulnerable. Most importantly, however, such modeling clearly identifies intelligence data requirements, collection priorities, and the operational essential elements of information.

The information and experience gathered in such a modeling exercise will additionally serve to identify techniques, technologies, and processes that could provide a significant defensive advantage to the information systems in question. Paradigm shifts such as distributed decisionmaking, groupware, and collaborative environments conceptually leapfrog both security controls and security configuration management. Methods carefully crafted to secure computers that stood alone have been shown to be wholly inadequate when computers are networked. The intricacies associated with information warfare simply add one or more dimensions of complexity to this situation.

GETTING THERE

The Navy must be able to perform assigned missions in the year 2035 with appropriate technologies, procedures, and capabilities. Apropos the information environment, this includes:

- Defending against attacks on own information technology resources;
- Conducting offensives against adversary's information technology resources; and
- Using information operations in ways that are neither clearly offensive nor defensive in nature to support using other tools, technologies, and procedures or to achieve desired mission outcomes.

Performing these operations is complicated by the following elements:

- The borders of information technology will not stop at the ship's hull, but continue past the hull to locations that the warfighter will have neither control over nor possibly even knowledge of;
- Cooperative engagement resources, such as the arsenal ship, must be included in the comprehensive offensive and defensive posture assessment; and
- The increasing incorporation of information technology into every facet of operations can be expected to include wearable computers, personal protection measures (to include medical developments, such as "smart" skin applications) as well as integrated control applications.

Implicit in an assumption of ubiquitous information systems, technology, and resources are the following:

- Useful and pervasive defenses of the information infrastructure and of information content;
- Potential offensive capabilities for use against the adversary's information infrastructure and/or the adversary's information content;
- The ability to command and control information technology defenses and offenses;
- The developed intellectual basis for information operations, specifically tactics and doctrine;
- The availability of intelligence to support the use and development of information technology resources, offense, and defense; and
- The availability of surveillance and reconnaissance data to support real-time adjustments to the information posture.

For the future naval forces to be able to coordinate and operate the range of required capabilities, both explicit and implicit, a range of integrated processes associated with information operations and warfare must be in place and operational. These processes include the following:

- Requirements identification and prioritization,
- Research and development,
- Acquisition,

- Interface negotiation and resolution,
- Equities resolution,
- Vulnerability assessments,
- Intelligence processes,
- Metrics collection and analyses, and
- Training and education.

The development and acquisition of technology without such supporting processes would result in less useful capabilities; as with all information technologies, the role of the people and the organizational constructs within which the technologies are implemented are critical elements in the success or failure of those technologies to achieve their specific goals.

As with any road map, it is important to know not only what the desired end point is, but also where you are starting from. Critical elements of the current posture that will affect any attempt to meet the Navy's goals in developing a competent information operations and warfare capability are discussed briefly below.

1. *Information security resources and standards*. The current level of expenditure for the Department of the Navy in information security is less than 2 percent of the Navy Department's acquisition budget, having been on a steady decline since the late 1980s. Specific expenditures on security for information-intensive programs (virtually every program today) differ from program to program according to the priorities of the program manager. Required milestones, such as certification and accreditation of information systems, are often waived or overlooked. This is inadequate. The report from the Joint DOD/Director of Central Intelligence (DCI) Security Commission, published in 1994, entitled *Redefining Security*, stated:

> In reviewing the best practices of government and industry, the Commission finds that an investment strategy that allocates five to ten percent of the total cost of developing and operating information systems and networks is appropriate and needed to ensure that those systems and networks are available when needed and safe to use.[4]

In keeping with the importance of information to the Navy, it would be prudent to measure and assess the level of expenditures for information security for appropriateness and enforce currently imposed information security requirements.

A critical element of emerging information security engineering is protecting against induced vulnerabilities associated with large systems integration

[4] Joint Security Commission. 1994. *Redefining Security, A Report to the Secretary of Defense and the Director of Central Intelligence*, Washington, D.C., February 28, pp. 108-109 (available online: http://cscr.ncsl.nist.gof/secpubs/jscrprt.txt).

and architecture standards. Initiatives such as the joint technical architecture (JTA) are appealing due to their promise of increased interoperability between Services and potential plug-and-play capabilities. However, there are dangers lurking in such efforts. Increased homogeneity of system components makes the system as a whole susceptible to a smaller set of attacks (or inherent flaws), whereas heterogeneity of systems makes a potential adversary's task much more complicated. Features designed to provide redundancy for critical systems may in fact not provide resiliency—if the redundant system is made up of the same components as the primary system, it may well be vulnerable to the same kind of attack.

2. *Offensive and defensive coordination*. An increasingly artificial distinction between the communities providing and operating the offensive and defensive elements of information operations stands in the way of developing truly operational capabilities. While there are real reasons for keeping secrets, the efforts of the two communities must be rationalized from the beginning and coordinated in the execution. The appointment of an executive agent for IW for the Navy should help in this regard. Specific technological thrust areas that should be addressed as well in the pursuit of a truly operational capability are ones that allow the warfighter to control his resources and operate efficiently in pursuit of mission objectives. Regarding offensive capabilities, the lessons learned from various exercises indicate a serious disconnect between prioritized operations and available weapon systems. Regarding defensive capabilities, the practice to date has been one of installing patchwork information security fixes in what has been termed a "fire and forget" mode. Regarding the supporting intelligence, it is currently not possible to detect and identify attacks in real time, allowing the warfighter to marshal forces to defend against such attacks or to counterattack. Significant research efforts are under way that would support such capabilities. These research efforts should be encouraged, with the end goal of having a truly operational capability that the operators can use.

3. *Organization*. The first steps the Department of the Navy is taking to create an operational information warfare organizational structure are certainly the right things to do. These steps, which include the development of the information warfare training and education curriculum, the creation of the Fleet Information Warfare Center (FIWC), and the designation of an executive agent for information warfare for the Navy Department, must be supported. In an era when the dependence on information and the promise of information-based operations are so obvious, fiscal and personnel shortfalls can only cost in the long run, both in terms of dollars and potentially in terms of lives lost. Arguments that increased funding for the information operations arena will lead to shortfalls in other warfighting areas must be analyzed and addressed proactively. If the promise of information operations is to be achieved, it will not be with poorly supported organizations and capabilities.

SUMMARY

The Department of the Navy must be able to manage and defend its information posture, including its information vulnerability, in the coming era of prolific information gatherers and promulgators. While doing this, the Navy Department must be able to deny information to adversaries as well as manipulate and/or attack it.

There are technology thrust areas that, if pursued, would provide the Department of the Navy with significant capabilities in information operations and information warfare. These technology thrust areas are based on the estimated evolutionary path of the global information environment in which the Navy Department will operate.

These capabilities must include both the content and infrastructure aspects of information.

None of this is inexpensive. There is clearly a tradeoff between the technological investments required to fully exploit the potential of IO and IW and the ongoing capitalization requirements of the more conventional platforms and weapons systems. The Navy Department must make these difficult tradeoffs to lay a foundation for its future ability to use information and information systems to support naval operations.

6

Strategy for Achieving Information Superiority

CONCLUSIONS

In summary, the Department of the Navy must recognize the significance of and critical dependence on information technologies and systems for future naval forces and elevate information superiority to a warfare area. The Department of the Navy must establish an integrated organizational structure with the responsibility for planning, programming, and budgeting for all information systems not unique to individual platforms or weapons. Career paths and educational programs must be established within this warfare area to provide incentives and rewards for the personnel involved.

Information superiority will be achieved only when a robust, seamless, and secure information infrastructure is established to support naval forces and provide them with the necessary information content in a timely and interpretable manner. The information infrastructure will be based largely on commercial systems and services, and the Department of the Navy must ensure that these systems are seamlessly integrated and that the information transported over the infrastructure is protected and secure. Network integration, components for robust communications links, development of adaptive transport protocols, and the development of intelligent service application software agents are critical to allow for establishing a seamless information infrastructure based on commercially developed systems and services and as such must be supported by the Navy Department and DOD.

As important as the infrastructure is the content of the information transported over that infrastructure. The information content will be established from multiple sensors and intelligence systems. With the explosion of information

systems globally, new sources of information and intelligence will emerge as information flows across the global commercial infrastructure. Commercial space-based imaging systems will provide timely submeter imagery worldwide. In addition to these commercial space-based assets and the significant information produced by National systems, the Department of the Navy must invest in unique radar and electro-optical sensors that will meet requirements for continuous coverage of the tactical battle space and allow for long-range precision targeting against all targets.

This expanding set of sensor systems will generate large databases that must be organized, accessed, interpreted, and presented in a time frame and format useful to the warfighter. Information content, understanding, and recognition theory are critical technology areas that will be increasingly important in an information-rich society, but there are many developments that must be supported by the DOD and Department of the Navy. In particular, database mining algorithms, sensor data fusion, and development of techniques for automatic target recognition must be supported.

The information infrastructure and the information content within that infrastructure must be protected, and U.S. forces must also be capable of denying an adversary access to the multiple sources of information available within the global commercial marketplace.

RECOMMENDATIONS

This volume reports on the panel's discussions of the future dependence of naval forces on information systems and the need to achieve information superiority to ensure the success of future warfighting strategies. It presents what the panel considers to be the characteristics of a robust information infrastructure and the information content carried to the warfighter over the infrastructure. It also discusses the sensor technologies and systems necessary to produce the data that will be processed, mined, and interpreted to generate the necessary information content, as well as the criticality of maintaining the security of the information infrastructure and the information flowing within those systems. The Navy Department C^3 staff organizations have traditionally focused on communications, computers, and data links. What is missing are sophisticated coordination of the specifications for organic and remote sensors, information networks, and precision weapons; understanding of the reliance that can be placed on National and theater sensors; and the appropriate investment balance among these components, not only of the entire sensor-to-shooter chain, but also spanning the spectrum from preparation of the battlefield to battle damage assessment. As an outgrowth of those discussions, the panel draws some specific conclusions and makes recommendations throughout the report.

The panel makes the following specific set of recommendations related to information in warfare and U.S. ability to achieve *information superiority.*

1. Establish and treat *information superiority* as a warfare area. Provide a mechanism for coordinating all Navy Department command, control, communications, computing, intelligence, surveillance, and reconnaissance (C^4ISR) resources, requirements, and planning.

A mechanism must be found to coordinate all aspects of information superiority across both Navy and Marine Corps C^4ISR endeavors, giving due consideration to the evolving missions for naval forces and to current and future capabilities for ISR performed by other Services and agencies. If established, such a mechanism could greatly enhance the capability of joint operations with other services. Except for dedicated organic intra-platform-specific systems, all resources, requirements, and planning for information systems—including architecture, nodes, links, networks, combat systems, and sensors—must be under the purview of that mechanism.

2. Encourage information superiority careers. Educate all officers, regular and reserve, about the information technologies, resources, and systems needed to support future Navy and Marine Corps operations; define a cadre of specialists; and identify a career path to flag/general officer rank.

3. Adopt commercial information technology, systems, and services wherever possible. Develop technologies only for special Navy and Marine Corps needs such as low-probability-of-intercept communications and connectivity to submerged platforms.

Where feasible, transmit Navy traffic through commercial systems or use commercial satellites with transponders and terminal equipment optimized for naval systems. When necessary, develop technologies to fit naval special needs such as those for multiband, multifunctional antennas; communications to undersea platforms; and low-probability-of-intercept and antijam-capable communications systems.

4. Modernize information systems and services aggressively. Strive to involve operational users, research commands, and acquisition organizations in a cohesive relationship that allows the continued rapid insertion of advanced information systems for use by Navy and Marine Corps forces.

The Navy Department should continue to modify and adapt the acquisition system, in collaboration with the warfighter, to allow accelerated demonstrations of advanced information technologies and the rapid fielding of new information systems. Where feasible, it should adopt commercial systems and adapt naval applications to their capabilities, rather than develop service-unique systems.

5. Focus information infrastructure R&D. Make integration of diverse commercial services and DOD-unique links a primary focus of information infrastructure and network research and development.

The Navy Department should pursue selected R&D focused especially on cross-network interoperability, involving commercial-to-military communication and interoperability, civil-to-military and military-to-military, such that seamless integration and transfer between these networks is easily achieved (air and space

communications to submarines is a good example). This cross-network technology R&D should incorporate both terrestrial wire and fiber, satellite relay, and tactical wireless (radio frequency [RF]) networks that allow shore-to-ship, ship-to-ship, air-to-ship, and ground-to-ground network interoperability.

6. Manage data sources. Establish a clear policy designating responsibility in the Navy Department for identifying, organizing, classifying, and assuring all relevant information sources that permit information extraction and communication from multiple remote locations. Invest in research on and development of tools and techniques to facilitate this shared information environment.

Ensure timely and convenient access to all relevant information sources by naval assets. Invest in R&D to enable interoperability and remote access to information and to develop tools and techniques such as intelligent software agents that facilitate creation of a warfighter-friendly shared information environment. Such an environment will include maritime-specific databases and mirroring, and will reflect awareness of emerging information providers and vigilance in assessing and maintaining database quality.

7. Extract relevant information and knowledge. Adopt commercial data-mining technology for naval applications and pursue a theory of information understanding and apply it to target recognition.

Establish naval expertise and fund data-mining technologies from commercial technologies adopted for naval applications. In conjunction, emphasis should be placed on stimulating advances in recognition theory for the extraction of critical understanding and information. This should include enhanced attention to automatic target recognition (ATR) applications, force structure analysis, fusion methods, human-machine interfaces (HMIs), and smart databases and logistics support.

8. Exploit commercial sensing. Consider commercial space-based imaging systems and tools for exploiting them, as well as mechanisms for distributing data, in support of naval applications.

The DOD and the Department of the Navy should adopt acquisition strategies that take maximum advantage of the capabilities provided by commercially available space- and airborne imaging systems and should seek to exploit spin-offs of commercially developed sensor technology for application to military-unique applications.

9. Exploit National and joint sensors. Provide online/direct connectivity to naval platforms and Marine Corps units to support long-range and precision-guided munitions.

The Department of the Navy must continue to integrate naval sensor systems with National and joint systems to provide near-real-time wide-area surveillance and target identification in support of force projection ashore. Investment should be made to provide digital connectivity and direct downlinks to support robust C^4ISR, as well as sensor-to-shooter architectures for long-range and precision-guided munitions. When early external support cannot be ensured,

the Department of the Navy should consider the development of organic sensors to sustain *Forward ... From the Sea* dominance.

10. Make information warfare operational. Integrate defense and offense and develop needed technology, systems, tactics, tools, and intelligence support.

To develop the capabilities required for information warfare in 2035, the Department of the Navy should continue to make information warfare activities operational by integrating defensive and offensive elements at the control of the warfighter and by investing in the development of specific technology for support of countermeasures and defensive capabilities, offensive tools and tactics, and intelligence capabilities.

APPENDIXES

A

Terms of Reference

CHIEF OF NAVAL OPERATIONS

28 November 1995

Dear Dr. Alberts,

In 1986, at the request of this office, the Academy's Naval Studies Board undertook a study entitled "Implications of Advancing Technology for Naval Warfare in the Twenty-First Century." The Navy-21 report, as it came to be called, projected the impact of evolving technologies on naval warfare out to the year 2035, and has been of significant value to naval planning over the intervening years. However, as was generally agreed at the time, the Navy and Marine Corps would derive maximum benefit from a periodic comprehensive review of the implications of advancing technology on future Navy and Marine Corps capabilities. In other words, at intervals of about ten years, the findings should be adjusted for unanticipated changes in technology, naval strategy, or national security requirements. In view of the momentous changes that have since taken place, particularly with national security requirements in the aftermath of the Cold War, I request that the Naval Studies Board immediately undertake a major review and revision of the earlier Navy-21 findings.

The attached Terms of Reference, developed in consultation between my staff and the Chairman and Director of the Naval Studies Board, indicate those topics which I believe should receive special attention. If you agree to accept this request, I would appreciate the results of the effort in 18 months.

Sincerely,

J. M. BOORDA
Admiral, U.S. Navy

Dr. Bruce M. Alberts
President
National Academy of Sciences
2101 Constitution Avenue, N.W.
Washington, D.C. 20418

Enclosure

TERMS OF REFERENCE

TECHNOLOGY FOR THE FUTURE NAVY

The Navy-21 study (Implications of Advancing Technology for Naval Warfare in the Twenty-First Century), initiated in 1986 and published in 1988, projected the impact of technology on the form and capability of the Navy to the year 2035. In view of the fundamental national and international changes -- especially the Cold War's end -- that have occurred since 1988, it is timely to conduct a comprehensive review of the Navy-21 findings, and recast them, where needed, to reflect known and anticipated changes in the threat, naval missions, force levels, budget, manpower, as well as present or anticipated technical developments capable of providing cost effective leverage in an austere environment. Drawing upon its subsequent studies where appropriate, including the subpanel review in 1992 of the prior Navy-21 study, the Naval Studies Board is requested to undertake immediately a comprehensive review and update of its 1988 findings. In addition to identifying present and emerging technologies that relate to the full breadth of Navy and Marine Corps mission capabilities, specific attention also will be directed to reviewing and projecting developments and needs related to the following: (1) information warfare, electronic warfare, and the use of surveillance assets; (2) mine warfare and submarine warfare; (3) Navy and Marine Corps weaponry in the context of effectiveness on target; (4) issues in caring for and maximizing effectiveness of Navy and Marine Corps human resources. Specific attention should be directed, but not confined to, the following issues:

1. Recognizing the need to obtain maximum leverage from Navy and Marine Corps capital assets within existing and planned budgets, the review should place emphasis on surveying present and emerging technical opportunities to advance Navy and Marine Corps capabilities within these constraints. The review should include key military and civilian technologies that can affect Navy and Marine Corps future operations. This technical assessment should evaluate which science and technology research must be maintained in naval research laboratories as core requirements versus what research commercial industry can be relied upon to develop.

2. Information warfare, electronic warfare and the exploitation of surveillance assets, both through military and commercial developments, should receive special attention in the

review. The efforts should concentrate on information warfare, especially defensive measures that affordably provide the best capability.

3. Mine warfare and submarine warfare are two serious threats to future naval missions that can be anticipated with confidence, and should be treated accordingly in the review. This should include both new considerations, such as increased emphasis on shallow water operations, and current and future problems resident in projected worldwide undersea capability.

4. Technologies that may advance cruise and tactical ballistic missile defense and offensive capabilities beyond current system approaches should be examined. Counters to conventional, bacteriological, chemical and nuclear warheads should receive special attention.

5. The full range of Navy and Marine Corps weaponry should be reviewed in the light of new technologies to generate new and improved capabilities (for example, improved targeting and target recognition).

6. Navy and Marine Corps platforms, including propulsion systems, should be evaluated for suitability to future missions and operating environments. For example, compliance with environmental issues is becoming increasingly expensive for the naval service and affects operations. The review should take known issues into account, and anticipate those likely to affect the Navy and Marine Corps in the future.

7. In the future, Navy and Marine Corps personnel may be called upon to serve in non-traditional environments, and face new types of threats. Application of new technologies to the Navy's medical and health care delivery systems should be assessed with these factors, as well as joint and coalition operations, reduced force and manpower levels, and the adequacy of specialized training in mind.

8. Efficient and effective use of personnel will be of critical importance. The impact of new technologies on personnel issues, such as education and training, recruitment, retention and motivation, and the efficient marriage of personnel and machines should be addressed in the review. A review of past practices in education and training would provide a useful adjunct.

9. Housing, barracks, MWR facilities, commissaries, child care, etc. are all part of the Quality of Life (QOL) of naval personnel. The study should evaluate how technology can be used to enhance QOL and should define militarily meaningful measures of effectiveness (for example, the impact on Navy readiness).

10. The naval service is increasingly dependent upon modeling and simulation. The study should review the overall architecture of models and simulation in the DoD (DoN, JCS, and OSD), the ability of models to represent real world situations, and their merits as tools upon which to make technical and force composition decisions.

The study should take 18 months and produce a single-volume overview report supported by task group reports (published either separately or as a single volume). Task group reports should be published as soon as completed to facilitate incorporation into the DoN planning and programming process. An overview briefing also should be produced that summarizes the contents of the overview report, including the major findings, conclusions, and recommendations.

B

The Navy and Satellite Communications

INTRODUCTION

The U.S. Navy, with its global sea-based operations, has always had to depend on electromagnetic communications. At first, of course, it employed optical frequencies (flags and lights), but early in the 20th century the Navy turned to radio and pioneered its early use. Working closely with industry, the Navy developed the technology for low- and medium-frequency transmission. RCA (then the Radio Corporation of America) was formed at the request of the Navy to provide a commercial radio service with David Sarnoff, a former Marine radio operator, at its helm. After World War I, the infant Naval Research Laboratory (NRL), under the guidance of Thomas Edison, embarked on a highly productive research effort in radio propagation, which developed a quite novel technique for radio detection and ranging, called "radar."

As the space age dawned in the 1950s, the U.S. Navy was highly experienced in radio technology and operations and prepared to utilize satellite communications. Indeed, the Navy can claim the first operational use of an Earth-orbiting satellite for communications—six years before Sputnik!

EARLY SATELLITE COMMUNICATIONS

Navy Satellite Communications

In 1951, NRL demonstrated the feasibility of bouncing radio signals off Earth's natural satellite, and in July 1954 actually transmitted the first voice

message over the Earth-moon-Earth path. The Navy then established an operational link between Pacific fleet headquarters in Hawaii and the Chief of Naval Operations (CNO) in Washington, D.C., carrying 16 channels of 60 words-per-minute ultrahigh-frequency (UHF) teletype for periods of 4 to 7 hours each day (depending on the moon's declination). As satellite communications systems go, moon relay rated fairly low on capacity and data rate, but extremely high on reliability—with negligible launch cost.

In 1962, the U.S. Navy took a significant step forward, building the first satellite communications ship, the USNS *Kingsport,* mounting a 30-foot stabilized antenna to provide a mobile terminal capability for the National Aeronautics and Space Administration's (NASA's) Syncom satellite. *Kingsport,* in the harbor of Lagos, Nigeria, relayed the first telephone call ever over a geostationary satellite, from President Kennedy via the Syncom II satellite. *Kingsport* later provided communications services in the Pacific and Indian Ocean areas for several years in support of tracking and recovery operations for NASA's Gemini program.

Early Experimental Programs

Within a year after the first Sputnik, the Department of Defense (DOD) and NASA initiated a number of experimental satellite projects that set the stage for operational military and civilian systems.

Score and Courier, developed and launched by DOD in 1958 and 1960, respectively, were the first communications satellite experiments. They demonstrated that delicate and complex electronic equipment could survive the trauma of launch and could operate in orbit.

NASA's entry was Echo, a 30-meter-diameter metal and plastic balloon, launched in 1960 to demonstrate passive satellite communications. Echo carried the first transoceanic satellite signal from Bell Laboratories in New Jersey to the French Communications Center in Paris.

Telstar, a medium-altitude satellite developed by AT&T Bell Laboratories and launched in 1962, was the most famous experimental satellite—its technical contributions so significant and its impact on the public so great that its name for a while became generic for "communications satellite." It was the first satellite to use a traveling wave tube (TWT). Significantly, Telstar received at 6 GHz and transmitted at 4 GHz, bands that later were assigned to commercial service and used by INTELSAT and all other fixed-service systems during the 1960s and 1970s. Telstar carried the first live television from the United States to England and France.

NASA's Relay satellite, a medium-altitude system like Telstar, launched a few months later, introduced additional technologies and provided extensive communications links, including the first between the United States and Japan.

NASA's Syncom satellite, built by Hughes and launched in 1963, was prob-

ably the single most important step in the development of satellite communications. It was the first satellite placed in geostationary orbit and became the model for many generations of operational spacecraft to follow.

Other early experimental satellites that deserve mention include the six NASA advanced technology satellite (ATS) series and the DOD leading-edge services (LES) and tactical satellites (TacSats), all of which made important technical contributions in developing spacecraft subsystems, Earth stations, and transmission systems and in opening up new frequency bands (specifically UHF, L, C, X, and Ka-bands). All of this experimental satellite work, conducted by the U.S. government throughout the 1960s and into the early 1970s, made military and commercial satellite communications possible and led to a thriving international industry.

The Navy participated in many of these programs, developing and testing terminals, multiple access, fleet broadcast, and antijamming technology.

Early Commercial SatCom

In July 1961, President Kennedy issued a policy statement, declaring that the United States would develop a global satellite communications system, not through the government or the monopoly carrier, AT&T, but through a new commercial entity, and with international cooperation. Following the presidential lead, the U.S. Congress passed the Communications Satellite Act of 1962 to form Comsat Corporation. The United States then joined with 10 other nations to form the international body known as INTELSAT. And in April 1965, less than four years after the concept was suggested, the world's first commercial satellite, INTELSAT I, known as Early Bird, was launched, and operational telecommunications service inaugurated between North America and Europe. This first satellite link carried 240 telephone circuits at $32,000 per circuit-year compared with the single undersea telephone cable then existing, which carried only 150 circuits at about $100,000 each. The satellite also had a unique broadband capability, frequently demonstrated, to carry television across the ocean with the phrase "live via satellite."

TECHNOLOGICAL PROGRESS

From the start, technological and operational progress in commercial satellite communications was very rapid. By the end of its first decade, INTELSAT was well into the fourth generation of successively larger, more powerful satellites (Table B.1) providing global coverage, connecting hundreds of Earth stations, and carrying thousands of telephone circuits plus television and data.

With more powerful satellites came the opportunity to shrink the size of Earth stations that could then be customized to fit users' requirements—located on a rooftop, for example, or on a moving platform such as a ship or submarine.

TABLE B.1 INTELSAT Satellites

	INTELSAT I	INTELSAT IV	delta
First launch	1965	1971	6 years
Weight	38 kg	700 kg	18x
Power	40 W	700 W	17x
Bandwidth	50 MHz	400 MHz	10x
Capacity (circuits)	240	4,000	16x
Cost/circuit-year	$32,000	$1,200	–96%

Microwave technology moved ahead rapidly in the 1970s, bringing improved TWT and solid-state power amplifiers, microwave integrated circuits, and multibeam antennas. These technologies led to the development of domestic satellite systems in several countries—in Canada (1972), the United States (1974), and Indonesia (1976).

Mobile and Broadcast Services

It was obvious from the start that communications via satellite offered two exceptionally valuable capabilities:

1. *Mobility:* the capability to provide two-way communications to a moving platform—be it a ship at sea, airplane in flight, or automobile on the highway.
2. *Broadcast:* the capability to transmit to multiple receivers simultaneously over a wide area (as much as one-third of Earth's surface from a single geostationary orbit satellite).

These two capabilities were exploited to a limited extent early on in the INTELSAT system, but starting in the 1970s, separate systems were established to provide mobile and broadcast services.

A set of experiments demonstrating reliable ship-to-shore service via INTELSAT IV conducted in 1973 on the ocean liner *Queen Elizabeth II* stimulated interest in the U.S. Navy in filling the gap before its then delayed and overbudget Fleetsat system would be ready for launch. This led to Marisat, the first mobile satellite communications system, which was established in 1976 to provide UHF service to the Navy and L-band service to the commercial maritime community. The L-band capacity of Marisat was later incorporated into the INMARSAT system. This is an excellent example of a successful combined military-civil system.

INTELSAT, in the 1960s, provided the first capability to transmit television across the oceans for what was termed "occasional use," representing about 1 percent of INTELSAT's revenues. In the 1970s, U.S. domestic systems began

carrying full-time television across the country for the three networks then in existence. With the explosion of cable television in the mid-1970s and through the 1980s, domestic satellites came into demand to provide service to cable heads. This in turn introduced the possibility of many networks. Also, the opportunity was created for anyone, particularly in a remote area lacking over-the-air or cable service, with the expenditure of only a few thousand dollars, to obtain his own small Earth station. With that, he could receive the same channels carrying television traffic to cable head-ends. By the mid-1980s, there were over a million such terminals on farms, ranches, and even suburbs of major cities—and the broadcast satellite industry was born!

Europe and Japan beat the United States in introducing so-called direct broadcast satellites (DBSs). These satellites have enough effective radiated power to broadcast into a small dish (less than 1-meter aperture), easily mounted on a rooftop and costing a few hundred dollars. By 1992, there were an estimated 5 million DBS terminals in Europe and Japan. In the last two years, with the launch of DirecTV by Hughes Communications, each satellite carrying 75 digital television channels, the United States stepped ahead of the rest of the world technologically. There are now some 20 million DBS terminals worldwide, including a rapidly growing population throughout the Far East.

The Navy has helped foster defense-wide interest in a global broadcast service through such projects as Radiant Storm, which explored the use of small antennas with high-power Ku-band downlinks for broadcast distribution. The Navy introduced satellite broadcast in defense satellite communications with the creation of fleet satellites in 1972.

Digital Satellite Communications

Because power and bandwidth are such precious commodities in the geostationary orbit, satellite systems have led the way in one of the most important developments in telecommunications—the shift from analog to digital processing and transmission techniques. Digital techniques (e.g., pulse code modulation [PCM] coding, phase shift keying [PSK] modulation, time division multiple access [TDMA]) were rapidly developed and introduced in satellite communications systems starting in the mid-1970s, and installed in many systems in the 1980s, to provide efficient data compression, demand assignment, and multiple access systems.

COMMERCIAL SATELLITE COMMUNICATIONS TODAY

Satellite communications today is a big global business—exceeding $20 billion per year, including revenues from satellite-borne traffic and sales of spacecraft, launch vehicles, Earth terminals, and transmission equipment. All of these segments appear to be highly profitable, with various services—telephone, tele-

vision, and data; fixed, broadcast, and mobile—growing at annual rates of 10 to 40 percent. As the first and still the only significant commercial payoff from space, satellite communications continue to provide substantial return for every dollar invested in R&D.

More than 200 countries and territories are currently involved in satellite communications. INTELSAT alone has 140 member countries. Fifteen countries have significant industrial capacity related to satellite communications. There are some 30 national, regional, and international satellite communications systems in operation employing more than 200 satellites in geostationary orbit. Tens of thousands of large Earth stations ranging from 3 to 30 meters, more than 200,000 very small aperture terminals (VSATs) (1 to 3 meters), 20,000 shipboard terminals, and 20 million direct broadcast receiving terminals (less than 1 meter) are in operation, carrying voice, video, and data traffic to international capitals and remote villages, to ships at sea and aircraft in flight, around the globe and around the clock. Highly portable voice-grade transceivers the size of a laptop, selling for about $5,000, are now in use, with advanced systems planned for the late 1990s, promising hand-held units similar in weight and cost to a cellular phone.

Of the three satellite communications services—fixed, mobile, and broadcast—only the first may be considered really mature, growing at rates of 5 to 10 percent per year. Within the fixed service, telephone traffic seems to be flat or decreasing, television distribution is increasing slowly (offset somewhat by gains in transmission efficiency), and VSAT systems are increasing rapidly (but account for relatively little transponder capacity). Broadcast and mobile satellite services are growing rapidly, increasing numbers of terminals, amount of traffic, and revenues from 20 to 40 percent per year.

The next move in mobile systems will be to the use of hand-held units for what is being termed "personal service." This service may be provided by either a few large, powerful satellites in geostationary orbit or by a larger number of satellites in lower orbit (as noted in the following section).

LEO vs. GEO Systems

For three decades all commercial communications satellites have operated in geostationary orbit, which has several advantages, primarily that "one satellite makes a system." A geostationary orbit (GEO) spacecraft can provide greater communications capacity per pound in orbit or per unit of launch cost than can a set of low Earth orbit (LEO) spacecraft. Also, a GEO satellite's power and bandwidth may be configured to match communications requirements through the use of multibeam antennas and spot beams, weighted and shaped beams, and efficient demand assignment and multiple access techniques.

The advantages of LEO and medium Earth orbit (MEO) over GEO for communications satellites lie in decreased transmission delay time and full global

coverage. Also, whereas aperture size is limited for GEO satellites, LEO satellites can provide a greater flux density to a given small area on the ground, allowing use of smaller terminals. This is a very appealing argument for the use of LEO systems intended to communicate with hand-held terminals.

In the past, low- and medium-altitude satellites have been employed for remote sensing, for scientific measurements, and for certain military missions in order to get full global coverage (including the poles) and the highest possible resolution (for limited aperture size). These systems have used relatively few satellites and launches. The largest currently operating system is the Global Positioning System (GPS) with 24 satellites. There has been no government or commercial experience with large numbers of satellites in precisely spaced orbits as required in certain proposed systems (see next section).

LEO and MEO Systems

Four low- or medium-altitude (LEO/MEO) multiple-satellite L-band (and S-band) systems—Iridium, Globalstar, Odyssey, and ICO—are currently under development, each aimed primarily at providing mobile voice-grade service to hand-held sets. All are in direct competition with each other and with existing and proposed GEO mobile systems. The LEO/MEO systems are all going through the tortuous process of applying for licenses, requesting frequency applications, seeking investors, lining up international partners, organizing contract teams, conducting system and marketing studies, doing detailed design work, and letting construction contracts.

- *Iridium* is a system funded and under development by Motorola Satellite Communications, Inc., with Lockheed as the spacecraft builder. Its estimated cost is $3.4 billion.
- *Globalstar* is under development by Loral Qualcomm Satellite Services, Inc., and is estimated to cost $1.8 billion.
- *Odyssey*, proposed by TRW, Inc., is estimated to cost about $2 billion.
- *ICO.* INMARSAT conducted a set of system concept and design studies over the last five years under its "Project 21" to determine the optimum nature of a system for its entry into the personal service market. It split off an affiliate company in 1994 called ICO to build a system of 12 medium-altitude satellites in two orbital planes. It conducted a competition and recently awarded a contract to Hughes to build satellites. The ICO system is estimated to cost $2.6 billion.

Some major characteristics of the three systems mentioned above are shown in Table B.2.

All four of the LEO/MEO systems (Iridium, Globalstar, Odyssey, and ICO) are being proposed by competent and experienced organizations—three U.S. aerospace companies (Motorola-Lockheed, Loral, and TRW) and the interna-

TABLE B.2 Major Characteristics of Iridium, Globalstar, and Odyssey

	Iridium	Globalstar	Odyssey
Altitude	785 km	1,401 km	10,335 km
Constellation	6 x 11 = 66	8 x 6 = 48	3 x 4 = 12
Weight	680 kg	400 kg	1267 kg
Crosslinks	4 x 23 GHz	None	None
Data rate	4.8 kb/s	1.2-9.6 kb/s	1.2-9.6 kb/s
Multiple access	TDM	CDMA	CDMA
Processing	Switch & routing	None	None
Capacity	3,840 circuits	>2,800 circuits	2,300 circuits
Terminal price	$2,000 to $3,000	$750	<$500

tional INMARSAT consortium. All four systems appear to be technically feasible. However, all face technical problems, coupled with some level of financial, organizational, and/or political difficulties. It is not at all clear how many of the four will survive the development process, and if so, how well the survivor(s) can compete with each other.

These systems are potentially significant to naval operations because, while basically directed at land-based users, they inherently cover the broad ocean areas and the polar regions that may generate little commercial traffic. But the Navy can benefit from the low-cost access available through these systems for logistic and administrative traffic, including sailor access to direct-dial calls to home for quality of life improvement. In addition, these systems are built around very small, low-cost terminals, thereby making their adoption by the Navy cost-effective.

Competitive Services

It is important to note that all three services—fixed, broadcast, and mobile—have competitive terrestrial systems (Table B.3).

The claim for a role of satellites in the global information infrastructure currently being voiced by the satellite communications community generally emphasizes the wide-area coverage, the mobility, and the distance-insensitivity

TABLE B.3 Competitive Services

Service	Competitor	Satellite Advantage
Fixed	Optical fibers	Multinode networks
Broadcast	Cable networks	Wide-area coverage
Mobile	Cellular	Wide-area coverage

to cost that satellites provide. These capabilities give satellite communications an enormous and unchallenged advantage in the broadcast and mobile services. The networking advantages of satellites over cable as applied to the fixed service are somewhat more subtle (as treated in the following sections).

Fixed Service Future

Within the fixed service, sparkling new opportunities appear to lie in high-data-rate networks—the market created by the introduction of optical fiber cables into local and regional telecommunications systems. The question seems to be whether satellites will have a significant role in interconnecting these local and regional networks into national and international ones, or whether fiber will overwhelm the global information infrastructure.

The rapid growth in telecommunications around the globe is causing a demand for ever higher data rates. Many businesses today are subscribing to integrated services digital network (ISDN) service (64 kb/s), and corporate networks are going to T-1 (1.5 Mb/s). Research centers are requesting T-3 (45 Mb/s). National and international carriers (including the Internet backbone) are now employing OC-3 (155 Mb/s). "Gigabit testbeds" (such as those in the U.S. High Performance Computing and Communications program) are operating at OC-12 (622 Mb/s) and OC-48 (2.4 Gb/s), and advanced technology experiments are pushing to rates as high as 100 Gb/s.

Military requirements in almost all respects mirror commercial requirements. In some but not all cases military requirements lead civil applications. There is little doubt that the first decade of the next century will see military operational requirements emerge for all of these high data rates.

In the case of the Navy, high data rates will be needed for imagery and other sensor data that may be associated with cooperative engagement capability, cruise missile retargeting, video conferencing, medical services, and training using "virtual reality."

Networks

Satellites are bound to play an important role in future high-data-rate networks, as they have in networks at lower data rates. If several widely separated sites are to be interconnected, satellites can provide significant performance and cost advantages over cables. If many sites are to be connected, satellites win handily. Because of satellites' wide-area coverage, and their valuable demand-assignment and multiple-access capabilities, these advantages increase with:

- The number of nodes in the network,
- The distance between the nodes,
- The variation in traffic loading on network paths, and

- The existence of geographic or political boundaries between nodes in the network.

These four factors all contribute to the preference for satellite-based networks in transcontinental, transoceanic, and international service.

In addition to multinode networks, a traditional niche for satellites has been in "thin route" service, and they will undoubtedly be so employed in the future. Although it seems strange now to think of an OC-3 link as thin, when the world is girdled with multigigabit fiber-optic networks, links to remote areas carrying only 155 Mb/s will be considered thin—and will just as surely be carried by satellites then as they are today.

Satellites, with their multiple-access demand-assignment capabilities can provide great flexibility as well economy to networks. One satellite transponder, for example, may be used as a transmission channel between Italy and Canada at one instant of time, and then a millisecond later, between England and Mexico, adjusting rapidly to traffic loading.

This network advantage for satellite service is very clear in VSAT systems in which the national switched telephone system is bypassed. Examples are as follows:

- The General Motors Corporation has a 9,000-node VSAT network connecting its offices, factories, suppliers, and dealers.
- Many stores and hotel chains, even gas stations (e.g., Wal-Mart, Kmart, Sears, Holiday Inn, and Chevron) employ VSAT networks for administrative service, reservations, and credit card verification.

Current VSAT systems operate at low data rates (fractional T-1) but will inevitably move up the data rate scale. This same advantage will also exist at higher data rates; i.e., what is true at T-1 today will be equally true at 30 times the rate (T-3) tomorrow, and at 100 times the rate (OC-3) the day after. Indeed, calculations (by AT&T) show that for satellite service to be more cost-effective than terrestrial service between two sites in the United States, they need to be separated by 5,000 kilometers; for three sites, 3,500 km; four sites, 1,300 km; and five sites, only 800 km. Of course, for many sites, say 100 or more, the satellite's advantage is overwhelming.

Satellite-based networks have additional advantages in terms of mobility and transportability—factors that are important for video news coverage, emergency service, and military use. Satellite ground terminals may be installed much more quickly than cables can be laid. Incidentally, satellites can be, and often have been, used for restoral of cable services. The use of satellites in providing emergency communications after the Kobe earthquake was a striking example of this.

It is most likely, then, that satellite-based networks for high-data-rate digital transmissions will have their maximum use in multinodal, transcontinental or

international linkages, particularly when subject to dynamic loading and where cost, flexibility, or mobility are important considerations.

The High-Data-Rate Market

What will the future requirements for national and international high-data-rate service be? First, we can assume that some of the same services now being provided at medium rates, such as T-1 and T-3, will be provided at higher rates in the next decade, increasing by factors of 10 every few years. Also, we might note that since computer and communications technologies are merging and that computers are running faster and faster, data links will go to higher rates.

A driving force in high-performance networking today is the need for distributed processing in computationally intensive science, engineering, and military applications such as climate modeling, computational fluid dynamics, aircraft design, or battlefield information collection and analysis.

These applications will require interconnectivity among supercomputers, high-performance servers, large databases, and remote input/output. Many require distribution of interactive video (at tens of megabits per second). Some require multichannel video coupled with fast access to large remote databases and visualization—and these mean even higher rates, in the range of hundreds of megabits per second. Once the computing and communications capabilities have been combined and the networking technologies developed to serve science and engineering applications, their use in industrial and commercial applications will surely follow—and on a worldwide basis.

ACTS

NASA's Advanced Communications Technology Satellite (ACTS) represents a $700 million investment by U.S. taxpayers, and a return after two decades to government-sponsored satellite communications R&D. ACTS was launched in September 1993 after a 10-year development period and is operating successfully in orbit with 3 to 4 years of expected useful service life remaining. ACTS was originally intended to accomplish two objectives:

- Develop advanced technologies, and
- Demonstrate new applications.

ACTS has accomplished its first objective with flying colors. It has shown that its advanced technologies (Ka-band, microwave matrix switch, multiple hopping-beam antenna, baseband processor) work in orbit. ACTS is making excellent progress toward its second objective. It has already demonstrated its prowess at modest data rates, enabling experiments to be conducted in many fields—in banking, distance learning, telemedicine, and military and mobile service. But

ACTS' most significant set of demonstrations—those at a high data rate—are just getting under way.

ACTS has a unique capability, the value of which could not have been appreciated when ACTS was designed more than 15 years ago. By virtue of the bandwidth available to it at Ka-band, ACTS can transmit digital signals at rates of up to 1 Gb/s. With five newly developed high-data-rate terminals, ACTS is demonstrating its ability to transmit at SONET rates of 155 and 622 Mb/s (OC-3 and OC-12).

One of ACTS' most demanding experiments is in supercomputer networking, in which a Cray supercomputer at the NASA Goddard Space Flight Center in Maryland is being connected with another Cray at the Jet Propulsion Laboratory in California through the satellite at OC-3 (155 Mb/s). In another experiment, now in progress, the Keck telescope in Hawaii is being connected to the astronomical data processing facility at the California Institute of Technology to perform a set of experiments in remote facility control and data visualization and analysis. ACTS has also been used for mobile communications experiments in aircraft and land vehicles. In one demonstration, called Aries, ACTS carried seismic data used for oil exploration from a ship in the Gulf of Mexico to a petroleum research center using asynchronous transfer mode (ATM) at data rates of 2 Mb/s.

Commercial Ventures

The Navy encountered several problems during the Gulf War in disseminating large volumes of information to commands and ships at sea. In many instances, military communications had to be supplemented with commercial satellite communications units. Navy ships found commercial INMARSAT terminals to be more reliable and user friendly than military terminals. As a result of this experience the Navy embarked on several ventures to test and evaluate the use of commercial satellite communications technology and systems.

Starting in 1992, under a project known as Challenge Athena, a number of demonstrations have been conducted at T-1 (1.5 Mb/s) using INTELSAT C band services that have shown a considerable advantage over DSCS. The USS *George Washington* (CVN-73) and eight other capital ships have conducted demonstrations via commercial satellite communications in subjects such as the following:

- National primary imagery dissemination,
- Intelligence data and tactical imagery transfer,
- DSCS emergency communications restoral,
- Video teleconferencing,
- Telemedicine, and
- Dial-up telephone service ("sailor telephone").

Challenge Athena has provided a convincing demonstration to the Navy that:

- High-data-rate satellite communications links to ships at sea are extremely valuable; and
- Use of commercial satellite communications technology and systems is a cost-effective way to obtain reliable, high-quality, high-data-rate services.

In late 1996, an ACTS mobile terminal was installed aboard the USS *Princeton* (CG-59), an Aegis guided-missile cruiser, to demonstrate naval applications at 1.5 Mb/s. A primary purpose of this installation is to demonstrate the capability of loading the large Aegis missile database while the ship is at sea. Future plans as part of Project Aries are to use the NASA ACTS and tracking and data relay satellites (TDRS) to provide data links to ships at sea at 6 to 10 Mb/s at both Ku- and Ka-bands.

Over the years, the Navy has been the primary proponent of satellite broadcast services, stemming from the widespread use of HF fleet broadcast in earlier days. Because of this interest, a wide-band 20-GHz broadcast capability is being added to a future UHF follow-on (UFO) satellite for DOD use.

SUMMARY

1. Satellite communications is a dynamic, high-technology, international, commercially successful enterprise, capable of providing a wide variety of services, in a reliable, cost-effective manner, to users of many types.

2. Commercial satellite communications systems offer a wider array of services, some with higher performance, and most at lower cost than the Defense Satellite Communication System (DSCS) or other military satellite communications systems.

3. Commercially available mobile and broadcast satellite communications services offer extremely valuable cost-effective capabilities to the Navy.

4. Commercially available medium-data-rate satellite communications services (1.5 to 45 Mb/s) and high-data-rate services (>155 Mb/s) now being demonstrated offer the potential of new and innovative capabilities to the Navy.

C

Commercial Space-based Sensors

INTRODUCTION

The commercial remote sensing systems industry intends to provide Earth imaging information obtained worldwide. The recent report by the Brown Commission discusses the need by U.S. forces for "…information about the world outside its borders to protect its national interests and relative position in the world, whether as a Cold War 'superpower' or a nation that remains heavily and inextricably engaged in world affairs. It needs information to avoid crises as well as respond to them, to calibrate its diplomacy, and to shape and deploy its defenses."[1] Much of the information is available today from National intelligence capabilities, and the potential for commercial remote sensing systems to augment the information provided by National assets is high. Integrating National and commercial assets could in addition allow National assets to be designed for capabilities uniquely required by National security interests and allow more resources to be available for technology development. In the future, it will be possible to take advantage of commercial remote sensing systems and thereby provide a more robust capability for the forces of the future.

The data collected by commercial remote sensing companies will be used to supply products that generally can be categorized as imagery interpretive products (representative of Defense Intelligence Agency [DIA] and National Photo-

[1] Brown, Harold, and Warren B. Rudman. 1996. *Final Report—Preparing for the 21st Century—An Appraisal of U.S. Intelligence*, Commission on the Roles and Capabilities of the United States Intelligence Community (the Brown Commission), Washington, D.C. (available online: http://www.gpo.gov/int/report.html).

graphic Intelligence Center [NPIC] products today) and map products (similar to National Intelligence Mapping Agency [NIMA]-generated mapping, charting, and geodesy [MCG] products). The attributes of these products will vary considerably, as is discussed in detail below. The potential for applying information-rich data and the resulting base imagery to new and future naval requirements is significant. Commercialization will allow software vendors and companies working directly with the users of the data to expand this development process more rapidly and make it available at lower cost. In addition, many of the commercial applications are equally applicable to naval interests. For example, algorithms trained on specific crops for determining crop yields can be trained on ocean plant life, allowing better assessments of navigation potential near coastal waters. More precise land-coastal demarcation is possible through the use of high-resolution remote sensing data. Remote sensing data available to ships at sea about their regions of interest will enable ongoing mission planning. Remote sensing data also provide a better base image for future sensors whose data will then become more attractive and of potentially greater value when used in conjunction with accurate base imagery data. Hyperspectral sensor data and SAR data are examples of data from future sensors that are likely to be available commercially for the naval forces in the year 2035, and probably much sooner.

Current naval leadership perceives three areas that drive Navy objectives not just for today but for the future as well: (1) forward presence, (2) engagement, and (3) fight to win. Information available from commercial remote sensing systems can contribute to supporting each of these areas. Remote sensing data will allow the Navy to intelligently understand the potential for forward presence and to reduce vulnerability by making use of information-rich, timely data available directly to these forces. Engagement will benefit in being able to task the sensors directly and obtain remote sensing data within minutes for the area of interest. The fight-to-win effort will benefit from data available for planning attacks as well as for assessing the success of operations and evaluating of enemy engagements. In addition, because much of this data will be archived, use of archived data with new data will allow a more comprehensive assessment to be made worldwide as the perceived foreign military threat is projected. How efficiently and effectively the Navy makes use of these new commercial remote sensing systems and the seamless integration of these and other data into the information infrastructure will enhance the Navy's capability for the future.

ASSESSING COMPETING PROVIDERS

Performance

The performance of products offered by the U.S. commercial remote sensing systems business will generally be measurable by the following key product discriminators:

- *Accuracy*. How precisely objects can be located?
- *Resolution and image quality*. How clearly can the size and shape of objects can be determined?
- *Information content*. How much information can be derived?
- *Timeliness and dependability*. How current is the information, how rapidly can it be delivered, and how dependable is the source?

Accuracy

Horizontal metric accuracy refers to the ability to locate an object within a given radius from its actual location. This is the key parameter in determining the scale of maps that may be produced. The more accurate the system, the greater its capability to produce precision maps at a reasonable cost. Maps are an important segment of the remote sensing market. Precision accuracy is also critical in certain military applications.

The inherent metric accuracy of a satellite system determines whether ground control points (GCPs) are required to achieve the desired accuracy of the finished product and, if so, how many. GCPs are basically location data confirmed by surveying or other techniques. Inherently less accurate systems may be able to produce high-accuracy products, but with relatively greater numbers of GCPs. The more GCPs required, the greater the cost of the product and the longer it takes to produce.

Resolution and Image Quality

Resolution determines how clearly the size and shape of objects can be determined. For example, 1-meter imagery can detect objects as small as 1 meter in size. High-resolution imagery products will also have high image quality, with relatively low levels of error or distortion. This high quality results from the superior technical capabilities of integrating the sensor, satellite platform, and ground processing facilities.

One of the most difficult problems to overcome in creating a high-performance satellite imaging system is reducing distortions caused by the movement of the satellite or its components. Particularly at high resolutions in the range of 1 meter, the slightest irregularity in such movements will create serious distortions in the imagery produced.

Revisit frequency is, in turn, a function of the system design, and the altitude and agility of the satellite. Some announced satellite systems apparently plan to operate at a lower altitude in order to achieve 1-meter resolution with a smaller and cheaper satellite. However, a higher-altitude satellite provides a wider coverage area for a given resolution.

Information Content

The information content of an image refers to the amount and type of information that can be extracted. Panchromatic (black and white) images contain information represented in a range of brightness levels or gray-scales. The number of gray-scale increments available is an exponential function of the number of information bits contained in the data (dynamic range). Most satellite systems to date have been 8-bit systems, which produce only 256 gray-scale levels.

Timeliness and Dependability

Another important feature of any system is its ability to deliver current information to the customer quickly and reliably. The currency of information depends largely on the collection capacity of a system and how frequently the system can access a particular area on Earth's surface (revisit frequency). The currency of information also depends on the speed with which it can be retrieved from a satellite, processed into products, and delivered to the customer.

Price

Companies in the remote-sensing industry will achieve price leadership by meeting the technical requiremets of a broad array of customers and by producing products efficiently through the use of such technologies as highly automated digital image processing. The anticipated expansion of the total market offers the potential for additional cost efficiency.

The competitive position of commercial satellite systems providers in both the map and interpretive product markets will be affected by the following variables:

- The levels of accuracy that will satisfy large portions of the market for maps;
- The image quality, information content, and timeliness of availability of the interpretive products provided by existing and announced competitors;
- The capability for providing unique products such as those that combine the accuracy and resolution of 1-meter panchromatic images with the information content of multispectral images; and
- A level of technology and performance that contributes to broad market appeal, thus enabling a company to meet or beat the prices of other providers of space-based sensing systems for most products.

Capabilities of Announced Space-based Sensing Systems

Table C.1 summarizes the capabilities of the announced private high-resolution systems.

TABLE C.1 Summary of Private High-resolution Systems

System	Announced Launch Date	Resolution at Nadir	Accuracy	Information Content	Other Features and Comments
Space Imaging (SI)	Late 1997	Pan: 0.82 m MS: 3.28 m	1.5 m 1:2,400 with few GCP 1:24,000 w/o GCPs	11-bit 4-band MS	Altitude: 680 km FR: 750 km APPD: 1.82 APD: 442 s Pan-sharpened capability
Earth Watch (EarlyBird) (QuickBird)	Late 1997[a] Spring 2000	Pan: 1 m MS: 4 m	< 20 m[b] 1:24,000 with GCPs[c]	11-bit 4-band MS	Altitude: 470 km FR: 560 km APPD: 1.15 APD: 351 s Centralized operations

LEGEND: Pan, panchromatic; MS, multispectral; GCP, ground control point; FR, field of regard at 1-m resolution; APPD, average passes per day; APD, average pass duration.

[a]But see EarthWatch Satellites Launch Schedule (available online: www.digitalglobe.com/company/satellites.html).

[b]Gupta, V. 1995. "New Satellite Images for Sale," *International Security*, Vol. 20, No. 1, p. 102.

[c]It is not clear whether QuickBird can produce lower-map-scale products, and if it can, how many GCPs would be required.

IMAGERY PRODUCTS AND MARKETS

The overall remote sensing market is composed of users of two basic types of imagery products: map products and interpretive products.

Map Products

Map products provide information about the geographic location of objects on and features of Earth's surface, and they often serve as the base map for a geographic information system (GIS), providing a foundational coordinate system as well as topographic contour information. Commercial and civil governmental entities use map products for infrastructure development, land management, and natural resource development. Defense and intelligence agencies use map products for strategic and tactical planning and operations. Accuracy is the most important parameter in this market, although one or more of the other product discriminators listed above may be relevant, depending on the application. The commercial map product market has historically been dominated primarily by aerial firms, because they alone have been able to produce the necessary positional accuracy.

Interpretive Products

Interpretive products provide information concerning a number of surface features other than geographic location. These features range from attributes such as size, shape, and relative location, which are visually identifiable in panchromatic and multispectral imagery, to more complex information such as crop health, vegetation density, mineral distribution, chemical composition, or water turbidity.

The value of interpretive products lies mainly in the extent to which the image or image data can be interpreted to extract information. Interpretive products fall into two main categories: visual products and multispectral classification products. In visual products, information about the contents of a scene, including the shape, size, and orientation of individual objects and groups, is visually apparent to the human eye. Changes can be observed by comparing images taken at different times. Panchromatic (black and white) images have been the most common examples of visual interpretive products in the past. However, multispectral (color) products can be used to extract considerably more information than panchromatic products, and the ready availability of high-resolution multispectral images will increase recognition of the value of color in image interpretation and create new demand for this high-margin product.

In multispectral classification products, spectral response data is analyzed by computer to extract information and highlight distinctions not otherwise discernible by the human eye. These products have been used for such purposes as

determining soil conditions, distinguishing between different kinds of crops, assessing crop health, providing target identification, and evaluating road trafficability.

Defense and intelligence agencies are probably the largest users of visual interpretive imagery. These agencies currently obtain such imagery mainly from their own government systems. Interpretive products also have a wide range of actual and potential commercial and civil government uses, and it is expected that commercial and civilian government use of interpretive products to grow in the future.

Users of interpretive products are generally not as concerned about accuracy as they are about resolution, image quality, and information content. Timeliness and dependability are often also important to users of these products. These are the traditional products that National systems have provided for defense and intelligence purposes. However, in addition to high resolution, defense analysts also require high image quality, because distortions such as pixel response variation, banding, and streaking or smearing will significantly reduce their ability to interpret information with confidence. Greater information content allows more precise identification through the presentation of more refined contrasts in panchromatic imagery, and enables a broader range of analysis through the addition of multispectral information. Timeliness and dependability are also of great importance to military and intelligence users who monitor national security situations and therefore require the most current and most reliable information available. For certain military applications, such as targeting, accuracy at the level of meters is also important. Table C.2 shows the ground resolution at which a range of targets can be identified and analyzed.

POTENTIAL DEFENSE APPLICATIONS

The Navy should look on commercial remote sensing systems as a source of information complementary to that available through National technical means. With the advent of both 1-meter panchromatic and 4-meter multispectral data, the effective image resolution provided by commercial space-based sensing systems can aid the military in its intelligence and power-projection missions. A capability for next-generation systems to begin to undertake some of the indications-and-warning missions that have been accomplished by other systems would allow some level of National-systems queuing, resulting in more efficient use of their time. Capabilities for port monitoring and some directed shipping lane surveillance are available. With additional imaging resources, using commercial imaging for events that require situation assessment and mission planning, rather than redirecting National assets, might help in overcoming some of the resource limitations and consequent prioritization that have kept the military from having some of its remote sensing requirements fulfilled.

The four multispectral bands offered by most of the commercial systems,

TABLE C.2 Approximate Ground Resolution in Meters at Which Target Can Be Detected, Identified, Described, or Analyzed

Target	Detection[a]	General ID[b]	Pecise ID[c]	Description[d]	Technical Analysis[e]
Bridges	6	4.5	1.5	1	3
Communications					
Radar	3	1	0.3	0.15	0.015
Radio	3	1.5	0.3	0.15	0.015
Supply dumps	1.5-3	0.6	0.3	0.03	0.03
Troop units (in bivouac or on road)	6	2	1.2	0.3	0.15
Airfield facilities	6	4.5	3	0.3	0.15
Rockets and artillery	1	0.6	0.15	0.05	0.045
Aircraft	4.5	1.5	1	0.15	0.045
Command and control headquarters	3	1.5	1	0.15	0.09
Missile sites (SSM/SAM)	3	1.5	0.6	0.3	0.045
Surface ships	7.5-15	4.5	0.6	0.3	0.045
Nuclear weapons components	2.5	1.5	0.3	0.03	0.015
Vehicles	1.5	0.6	0.3	0.06	0.045
Minefields	3-9	6	1	0.03	—
Ports and harbors	30	15	6	3	0.3
Coasts, landing beaches	15-30	4.5	3	1.5	0.15
Railroad yards and shops	15-30	15	6	1.5	0.4
Roads	6-9	6	1.8	0.6	0.4
Urban areas	60	30	3	3	0.75
Terrain	—	90	4.5	1.5	0.75
Surface Submarines	7.5-30	4.5-6	1.5	1	0.03

SOURCE: U.S. Senate Committee on Commerce, Science, and Transportation, NASA authorization for fiscal year 1978, pp. 1642-1643; and *Reconnaissance Hand Book,* 1982, McDonnell-Douglas Corporation, p. 125. Adapted from Table 1 in Ann M. Florini, 1988, "The Opening Skies: Third-Party Imaging Satellites and U.S. Security," *International Security,* Vol. 13, No. 2, pp. 91-123.

[a]Location of a class of units, objects, or activity of military interest.

[b]Determination of general target type.

[c]Discrimination within target type.

[d]Size/dimension, configuration/layout, components construction, equipment count, etc.

[e]Detailed analysis of specific equipment.

specifically the blue and the near-infrared, should enable an added level of area evaluation and target detection and identification capability that is not possible with standard 1-meter or better panchromatic images. Combining the spectral data of the four separate bands with the increased spatial resolution of the panchromatic band should yield a greater ability to detect objects in the water and

find camouflaged vehicles around a landing area. Imaging of some degree of soil trafficability can also be performed with the aid of the near-infrared band, thus providing information to support an actual landing.

When these capabilities are combined with near-real-time tasking and data receipt capabilities, the DOD is a transportable ground terminal away from having access to a high-resolution imaging system directly in the field or aboard a ship. This capability would provide long-sought-after information timeliness to the warfighter.

D

Acronyms and Abbreviations

ACTD	Advanced concept technology demonstration
ACTS	Advanced Communications Technology Satellite
AEW	Airborne early warning
AI	Artificial intelligence
AOR	Area of responsibility
APD	Average pass duration
APPD	Average pass per day
ASIM	Automated System Intrusion Monitor
ATM	Asynchronous transfer mode
ATR	Automatic target recognition
ATS	Advanced technology satellite
BDA	Battle damage assessment
C^2	Command and control
C^2I	Command, control, and intelligence
C^3	Command, control and communications
C^4ISR	Command, control, communications, computing, intelligence, surveillance, and reconnaissance
CCD	Camouflage, concealment, and deception
CDL	Common data link
CEC	Cooperative engagement capability
CEP	Circular error of probability

CNO	Chief of Naval Operations
COTS	Commercial off the shelf
CVN	Nuclear-powered aircraft carrier
DARPA	Defense Advanced Research Projects Agency
DBS	Direct broadcast satellite
DDS	Defense dissemination system
DISA	Defense Intelligence Service Agency
DOD	Department of Defense
DSCS	Defense Satellite Communication System
ECM	Electronic countermeasure
EHF	Extremely high frequency
ELINT	Electronic intelligence
EO/IR	Electro-optical, infrared
FAA	Federal Aviation Administration
FIWC	Fleet Information Warfare Center
FOPEN	Foliage penetration
FPA	Focal plane array
GCCS	Global command-and-control system
GCP	Ground control point
GEO	Geostationary orbit
GIS	Geographic information system
GOPEN	Ground penetration
GPS	Global Positioning System
HDTV	High-definition television
HF	High frequency
HMI	Human-machine interface
HUMINT	Human intelligence
IFF	Identification friend or foe
IFOV	Instantaneous field of view
IO	Information operations
IP	Internet protocol
IPB	Intelligence preparation of the battlefield
IR	Infrared
ISA	Intelligent software agent
ISAR	Inverse synthetic aperture radar
ISDN	Integrated services digital network
ISO	International Organization for Standardization
ISR	Intelligence, surveillance, and reconnaissance
IVHS	Intelligent vehicle highway system
IW	Information warfare
JCS	Joint Chiefs of Staff
JTA	Joint technical architecture
JTIDS	Joint Tactical Information Distribution System

LAN	Local area network
LEO	Low Earth orbit (satellite)
LES	Leading-edge services
LIDAR	Light detection and ranging
LOS	Line of sight
LPI	Low probability of intercept
MCG	Mapping, charting, and geodesy
MEO	Medium Earth orbit (satellite)
MIDS	Multifunction information distribution system
MILSTAR	Military strategic and tactical relay
MRC	Major regional conflict
MTI	Moving target indicator
MWIR	Mid-wave infrared
NASA	National Aeronautics and Space Administration
NCA	National Command Authority
NEDT	Noise equivalent detection temperature
NIMA	National Intelligence Mapping Agency
NIR	Near-infrared
NPOI	Naval prototype optical instruments
NRL	Naval Research Laboratory
NSA	National Security Agency
OODA	Observe, orient, decide, act
OOTW	Operations other than war
OPAM	Optical phased-array modulator
PCM	Pulse code modulation
PCS	Personal communications system
PSK	Phase shift keying
PSTN	Public switched telephone network
RCA	Radio Corporation of America
RCS	Radar cross section
R&D	Research and development
RF	Radio frequency
ROEs	Rules of engagement
SAR	Synthetic aperture radar
SatCom	Satellite communications
SCR	Signal-to-clutter ratio
SIGINT	Signal intelligence
SINCGARS	Single-channel ground-to-air radio system
SNR	Signal-to-noise ratio
SPOT	Systeme Probatoire d'Observation de la Terre
STAP	Space-time adaptive processing
SWIR	Short-wave infrared
TacSat	Tactical satellite

TDMA	Time division multiple access
TDRS	Tracking and data relay satellite
TEL	Transporter erector launcher
T/R	Transmit/receive
TWT	Traveling wave tube
UAV	Unmanned aerial vehicle
UFO	UHF follow-on (satellite)
UHF	Ultrahigh frequency
URAV	Uninhabited reconnaissance aerial vehicle
VHF	Very high frequency
VMF	Variable message format
VPN	Virtual private network
VSAT	Very small aperture terminal