 ADB212393

(1)

Information Warfare Technologies: Survey of Selected Civil Sector Activities.

INSTITUTE FOR DEFENSE ANALYSES ALEXANDRIA VA

FEB 1996

Distribution authorized to U.S. Gov't. agencies and their contractors; Critical Technology; Administrative/Operational Use; Specific Authority; 21 Jun 96. Other requests shall be referred to Information Warfare Div., (J6K) Joint Staff, Director of C4 Systems, The Pentagon, Room 1C826, Washington, DC 20318-6000.

UNCLASSIFIED / ~~LIMITED~~

UNCLASSIFIED Copy ______

IDA DOCUMENT D-1792

INFORMATION WARFARE TECHNOLOGIES: SURVEY OF SELECTED CIVIL SECTOR ACTIVITIES

W. J. Barlow, *Project Leader*
R. D. Turner, *Deputy Project Leader*

February 1996

19960719 024

Prepared for
Director of Command, Control, Communications, and Computers (C4), Joint Staff

Distribution authorized to U.S. Government agencies and their contractors; Critical Technology; Administrative Operational Use; Specific Authority; 21 June 1996. Other requests must be referred to the Joint Staff.

INSTITUTE FOR DEFENSE ANALYSES
1801 N. Beauregard Street, Alexandria, Virginia 22311-1772

UNCLASSIFIED DTIC QUALITY INSPECTED 4 IDA Log No. H 95-47446

The work was conducted under contract DASW01 94 C 0054 for the Joint Staff. The publication of this IDA document does not indicate endorsement by the Department of Defense, nor should the contents be construed as reflecting the official position of that Agency.

UNCLASSIFIED

IDA DOCUMENT D-1792

INFORMATION WARFARE TECHNOLOGIES: SURVEY OF SELECTED CIVIL SECTOR ACTIVITIES

W. J. Barlow, *Project Leader*
R. D. Turner, *Deputy Project Leader*
J. W. Barnett
J. M. Boone
A. E. Brenner
G. L. Brown
J. L. Gerrity
W. T. Mayfield
R. D. Raines
R. S. Ross

February 1996

Distribution authorized to U.S. Government agencies and their contractors; Critical Technology; Administrative Operational Use; Specific Authority; 21 June 1996. Other requests must be referred to the Joint Staff.

IDA

INSTITUTE FOR DEFENSE ANALYSES
Contract DASW01 94 C 0054
Task T-I1-1349

UNCLASSIFIED

PREFACE

This document has been prepared to set forth the results of a technology survey requested by the Joint Staff (J6K) pursuant to tasking from the Joint Warfare Capability Assessment (JWCA) Information Warfare Technology Subgroup.[1]

The approach chosen to highlight the technologies is a collection of "Technology Overview" survey forms using a format specified by the Joint Staff. The Institute for Defense Analyses (IDA) selected 56 technologies that are briefly described with regard to their potential long-term usefulness to Information Warfare applications. A more complete evaluation of a subset of the most promising technologies is provided in parallel IDA Paper P-3157, *Information Warfare: Selected Long-Range Technology Applications*.

The IDA study team consisted of Mr. William J. Barlow (Project Leader), Dr. Robert D. Turner (Deputy Project Leader), Dr. John W. Barnett, Mr. John M. Boone, Dr. Alfred E. Brenner, Dr. Gerald L. Brown, MG John L. Gerrity (USA, Ret.), Dr. William T. Mayfield, Dr. Renee D. Raines, and Dr. Ronald S. Ross. The team expresses its appreciation for the useful comments and constructive criticism provided by a technical review group chaired by Dr. David L. Randall and consisting of Mr. Harold A. Cheilek, Dr. Lane B. Scheiber, Dr. Richard E. Schwartz, RADM Grant A. Sharp (USN, Ret.), and Dr. John R. Shea.

1 *Technology Baseline for Information Warfare (IW) Vulnerabilities*, Contract DASW01-94-C-0054, Task Order T-I1-1349.

(This page is intentionally blank.)

CONTENTS

Appendixes

LIST OF FIGURES

LIST OF TABLES

(This page is intentionally blank.)

SUMMARY

A. THE TASK

At the request of the Joint Staff (J6K), IDA conducted a survey of emerging technologies in the academic and private sectors that could potentially have long-term payoffs in offensive or defensive Information Warfare (IW) applications. Over 11,000 data items on relevant technologies were identified from such sources as IDA's online data bases, World Wide Web searches, and the Defense Technical Information Center (DTIC) files. In addition, personal interviews and visits with several commercial and university sources, as well as the Defense Science Study Group (DSSG)[1] were conducted. Survey items were examined for their potential to contribute to Information Warfare capabilities; three criteria were used:

- Technologies providing performance enhancements
- Technologies providing entirely new functional capabilities
- Technologies essential to Defensive Information Warfare.

B. THE APPROACH

Using the foregoing criteria and simultaneously applying qualitative judgments with respect to physical feasibility, affordability, enhancement potentials, and relevance to IW, the study team refined the list of candidates to 56 technologies broadly categorized in the following IW areas:

Information Warfare Concepts:	9
Information Warfare Devices:	15
Information Warfare Software:	16
Information Warfare System Integration:	16

1 The DSSG is an Advanced Research Projects Agency (ARPA)-sponsored initiative and comprises some 60 current and former members of academic faculties from universities across the United States. They represent all the scientific and engineering disciplines and are focused on defense issues.

As requested by the Joint Staff, a separate "Technology Overview" sheet was prepared in a specified format for each of the 56 technologies and all are included in this document. The overviews include very brief statements regarding the technology's strengths, weaknesses, possible concepts of operation, and potential risks. This document does not attempt to provide detailed assessments or recommendations with respect to any of the 56 technologies. A parallel IDA paper is being prepared as noted below under "The Next Step" to more closely examine promising technologies.

C. THE RESULTS

Table 1 sets forth the results of the survey in the form of an Information Warfare Technology Matrix. The chosen technologies from the academic and private sectors are arrayed by functions and activity categories specified by the Joint Staff.

D. THE NEXT STEP

In preparing a parallel IDA Paper P-3157, *Information Warfare: Selected Long-Range Technology Opportunities,* the study team selected a subset of the 56 technologies to subject to a closer examination of potential payoffs, feasibilities, and risks. That paper also discusses a suggested framework in which to develop an IW technology baseline that includes both private sector and Government-sponsored technology activities.

Table 1. Information Warfare Technology Matrix

TECHNOLOGIES	Activity Categories		
	Links	Nodes	Human Factors
Concepts			
Immunological approach to change detection			X
Visualization of computer operations (algorithm animation)			X
Computing with DNA molecules			X
Stereo image processing			X
Natural evolution of machine codes: digital organisms			X
Semiotics			X
Mediology			X
Direct link from the brain to a computer	X		X
Computational sociology (social organization across extended networks)	X		X
Device Technologies			
Fiber optic undersea information network		X	
Microelectromechanical sensors	X		
Multiplexed communications with femtosecond laser pulses	X		
Electrooptical data storage on thin-film photoconductive materials		X	
Three-dimensional holographic storage of digital information		X	
Passive millimeter-wave camera		X	
Cesium vapor optical coorelator		X	
Blue-green diode lasers	X	X	
Gallium nitride blue and ultraviolet laser diodes	X	X	
Protein-based computers		X	
Optical flux-monitoring molecular beam epitaxy control system	X	X	
Quantum electronic computer device technology		X	
Modulable retroreflectors for coherent CO_2 laser communication	X		
Holographic visor displays		X	X
Integrated neural network for image detection and classification		X	
Software			
Real-time video insertion	X		X
Fractal information storage	X	X	
Speech recognition technology for hand-held computers			X
Distributed execution environment for high-performance parallel processing	X	X	
Image deblurring		X	
Multispectral imagery analysis		X	
Speech recognition for Windows-equipped personal computers			X
Soft-copy mapping system		X	X
Neural networks and fuzzy logic		X	X
Security architectures	X	X	
Distributed operating systems	X	X	
Distributed multimedia processing	X	X	X
Agent-oriented software/distributed artificial intelligence	X	X	X
Network intrusion detection	X	X	
Collaborative information sharing on the World Wide Web	X	X	X
Wavelet-based image compression	X	X	
System Integration			
Three-dimensional command-and-control information display		X	X
Synchronous optical network	X		
Wearable computer systems			X
3-D micro-imaging and visualization		X	X
High-performance multicomputer for 3-D graphics		X	X
Ultra-high-performance multicomputer for 3-D graphics		X	X
Haptic displays (force feedback for virtual environments)		X	X
Nanomanipulator		X	X
Optoelectronic head-tracker for head-mounted displays			X
Ultrasound visualization (augmented-reality echography display)		X	X
Electronic support measurement bistatic sensor technology		X	
Acoustic daylight ocean noise imaging system		X	
Laser beam propagation through atmospheric turbulence	X		
Integrated optical-digital correlation		X	
Real-time 3-D imaging and control		X	X
Directed search testbed and collaborative analysis and decision-making		X	X

(This page is intentionally blank.)

I. INTRODUCTION

A. BACKGROUND

This task was initiated by the Joint Staff's Joint Warfare Capability Assessment (JWCA) Information Warfare (IW) Technology Subgroup. The terms of reference prepared by the technology subgroup direct that selected participants:

> Research, analyze, and evaluate open information systems technologies within the DoD and private industry to baseline IW technology. Information technologies and leading edge research will be examined for both offensive and defensive applications. Additionally, a strategy must be provided that identifies, at the earliest possible stage, any emerging information technology and research developments within defense-oriented labs, federally funded research, and development corporations and private industry, which could have IW implications.

B. PURPOSE

The objective of this initial phase of work by IDA was to identify promising, relevant technologies from the academic and civil sectors and assess their long-term applications and payoffs for IW functions.

C. SCOPE

The range of technology development activities in the academic and civil sectors that are potentially relevant to IW applications is enormous. In order to develop a manageable perspective of the potential opportunities, it was necessary to limit the scope of the search efforts. As a first order approach, we attempted to identify examples on which we could be fairly specific about the kind of IW payoffs that a particular technological effort might support. Such payoffs tend to fulfill one of three general criteria:

- Significant enhancements to information collection, processing, or dissemination performance
- Entirely new information-handling functional capabilities
- Activities that might have important implications for defensive IW or information security.

While IDA did not make a systematic search of many generic technologies for information systems *per se*, a few are included in the survey because they seemed to meet the criteria just stated.

Finally, it was found that some technologies that are manifestly important for IW had little or no visibility in the civil sector. We feel certain that there are significant activities in this area, but accounts of the work are understandably not found in open sources.

D. CATEGORY STRUCTURES

Technologies yield benefits through processes that result in capabilities in the form of products or systems. The study team used a highly simplified concept of a technological process as a basis for sorting IW-related technologies into groups. The process begins with a *functional concept* for a new capability or a better way of realizing an existing capability. Depending on the elements needed, implementation of the concept may require new *device technology*, new *software*, or both. Ultimately, the process entails *integration* of one or more of these three elements into a *system*.

There is a natural ordering of these elements in time, which means that activities we have identified at the system integration level will more likely provide near-term benefits than those focused on device or software technology. Activities identified as being conceptual in nature represent opportunities for significant benefits over the longer term.

The Joint Staff has designated three system-oriented categories for Information Warfare technologies:

- *Nodes* are discrete functional elements that include sensors, facilities for data and information storage and processing, and automated devices for presentation, analysis, and decision making.
- *Links* are networks and communications for linking nodes to include transmission of unprocessed and processed sensor data, collection, and dissemination of information such as status/situation reports, archival data, and intelligence, and command messages or task assignments.
- *Human Factors* designate the visual, aural and/or tactile interfaces between automated equipment/machines and human operators/analysts/decision makers.

E. TECHNOLOGY SURVEY FORMAT

To aid in the development and use of a common approach to the technologies, the Joint Staff directed the use of a standard survey format illustrated by Table 2.

Table 2. Technology Survey Format

TECHNOLOGY SURVEY FORMAT
• Source • Points of Contact • Description • Who, What, Where, When, and How • Technology Strengths (Advantages Over Existing/Current Technology) • Technology Weaknesses (e.g., Feasibility, Difficulty, Costs) • Prototype Operations Concept (i.e., the IW Application) • Compatibility with Current Operating Environments • Technological Risks • Proprietary Aspects • Patents, Patent Applications, and Holders • Potential Limiting Operational Parameters • Commercial Availability

This document principally consists of a collection of these "Technology Overview" survey forms, arranged by the activity categories described above.

F. INFORMATION TECHNOLOGY RATE OF CHANGE

Underlying all discussions of Information Warfare applications is the enormous rate of change at which basic information technologies (e.g., computational, networks, infrastructure) are changing. Appendix A sets forth a brief history of these changes, traces the explosion in growth of computer technology, and forecasts some future developments of direct interest to IW functions.

G. DISTRIBUTED COMPUTER NETWORKS

The emergence of global computer-to-computer networks, initiated by the ARPA NET program, has important implications for all aspects of Information Warfare. Appendix B provides summary analyses of some major trends and issues, focusing on information security concerns.

(This page is intentionally blank.)

II. SURVEY OF TECHNOLOGIES IN THE ACADEMIC AND PRIVATE SECTORS

A. SAMPLING SURVEY

The world of information technology that is potentially relevant to IW is huge. Figure 1 gives some perspective of the problem of gathering data about that world. The IDA library began a search of online databases, and the results were immediately overwhelming. As illustrated by the figure, over 11,000 items were identified and the query for items related to information technology alone turned up almost 7,000 hits.

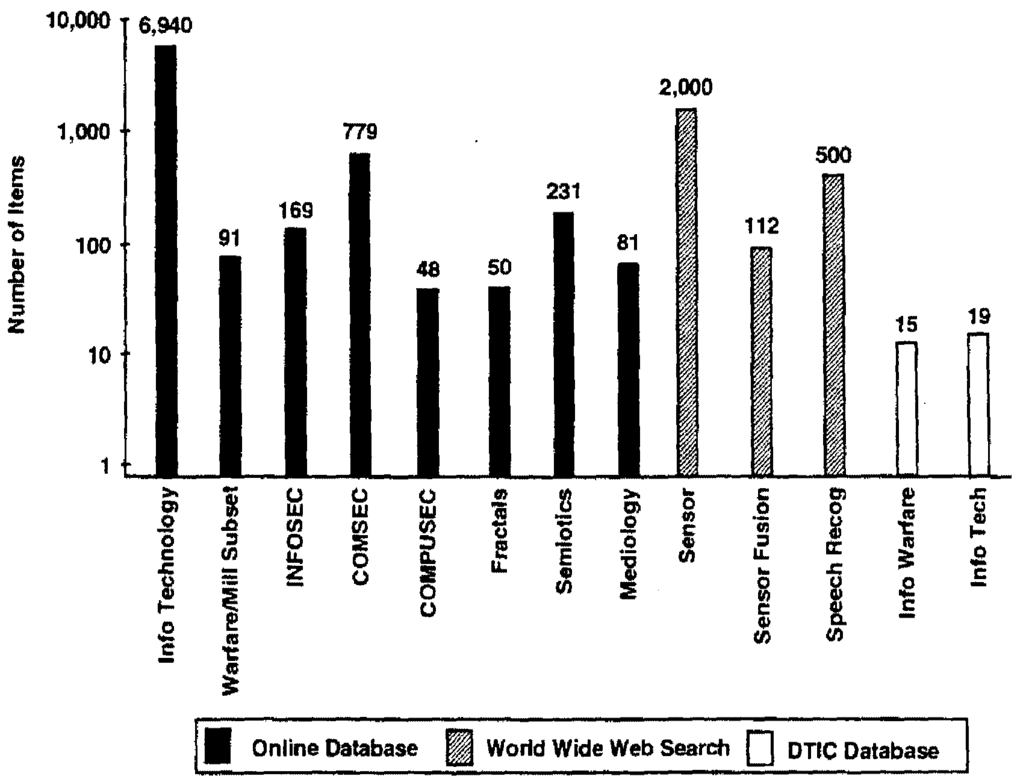


Figure 1. Sampling Information Warfare Technology

Much of the material turned out to be trade newsletter items, but even some of these were helpful in providing leads to new developments. When we narrowed the scope by specifying that the information technology had to be related to military or warfare applications, the list shrank to about 90 items. Note that this is still much larger than the return obtained from similar queries made of the Defense Technology Information Center database; but this is a risky approach because it would be possible to miss many interesting technologies where the developers have not explicitly recognized possible IW implications.

We also searched a number of sources that maintained home pages on the World Wide Web. Additionally, we used technology forecasts and scientific news digests to cover a lot of possibilities quickly and followed up on these leads by reviewing the original articles to obtain the kind of information that fit our search criteria.

B. LIMITING FACTORS

In order to develop a workable perspective of the opportunities relevant to IW, we elected to limit our search efforts as noted in Table 3.

Table 3. Limiting Factors

- ***Includes* Concepts and Emerging Developments that Could Influence or Drive Information Warfare Capabilities**
  - Performance Enhancements for Warfighting Information Systems
  - New Functional Capabilities for Warfighting Information Systems
  - Technology with Implications for Defensive IW
- ***Does Not Include* Generic Technologies for Information Systems**
  - Software Engineering Tools
  - Computer Chips and Chip Design and Fabrication Technology
  - Major Components (audio, RF, frequency standards, monitors)
  - Energy Sources
- ***Does Not Include* Technologies that Have Zero to Low Visibility in the Civil Sector**
  - Computer Virus Design
  - Tempest Protection and Sweep Technology
  - Eavesdropping Sensors and Intrusion Capabilities
  - Offensive IW Weapons

First we attempted to identify as many examples as possible where we could be fairly specific about the kind of IW payoffs that a particular technological effort might support: performance enhancements, new functionalities, and activities that might have important implication for defensive IW or information security.

We did not make a systematic search of the many generic technologies for information systems, but a few got into the package anyway because they seemed to meet the criteria just stated.

Finally, we found that some technologies that are manifestly important for IW have low visibility in the civil sector. We know, or are fairly certain, that there are significant activities in this area, but accounts of the work are usually not found in the open literature.

C. OVERVIEW OF TECHNOLOGIES

The survey selected some 56 technologies that are suggested as possessing long-term usefulness to Information Warfare applications. Tables 4 through 7 highlight the specific technologies in their applicable activity areas (i.e., concepts, devices, software, and systems integration).

Table 4. Technologies for Information Warfare Concepts

Concepts	Activity Categories		
	Links	Nodes	Human Factors
Immunological approach to change detection			X
Visualization of computer operations (algorithm animation)			X
Computing with DNA molecules			X
Stereo image processing			X
Natural evolution of machine codes: digital organisms			X
Semiotics			X
Mediology			X
Direct link from the brain to a computer	X		X
Computational sociology (social organization across extended networks)	X		X

Table 5. Technologies for Information Warfare Devices

Device Technologies	Activity Categories		
	Links	Nodes	Human Factors
Fiber optic undersea information network		X	
Microelectromechanical sensors		X	
Multiplexed communications with femtosecond laser pulses	X		
Electro-optical data storage on thin-film photoconductive materials		X	
Three-dimensional holographic storage of digital information		X	
Passive millimeter-wave camera		X	
Cesium vapor optical correlator		X	
Blue-green diode lasers	X	X	
Gallium nitride blue and ultraviolet laser diodes	X	X	
Protein-based computers		X	
Optical flux-monitoring molecular beam epitaxy control system	X	X	
Quantum electronic computer device technology		X	
Modulatable retroreflectors for coherent CO_2 laser communication	X		
Holographic visor displays		X	X
Integrated neural network for image detection and classification		X	

Table 6. Technologies for Information Warfare Software

Software	Activity Categories		
	Links	Nodes	Human Factors
Real-time video insertion	X		X
Fractal information storage	X	X	
Speech recognition technology for hand-held computers			X
Distributed execution environment for high-performance parallel processing	X	X	
Image deblurring		X	
Multispectral imagery analysis		X	
Speech recognition for Windows-equipped personal computers			X
Soft-copy mapping system		X	X
Neural networks and fuzzy logic		X	X
Security architectures	X	X	
Distributed operating systems	X	X	
Distributed multimedia processing	X	X	X
Agent-oriented software/distributed artificial intelligence	X	X	X
Network intrusion detection	X	X	
Collaborative information sharing on the World Wide Web	X	X	X
Wavelet-based image compression	X	X	

Table 7. Technologies for Information Warfare System Integration

System Integration	Activity Categories		
	Links	Nodes	Human Factors
Three-dimensional command-and-control information display		X	X
Synchronous optical network	X		
Wearable computer systems			X
3-D micro-imaging and visualization		X	X
High-performance multicomputer for 3-D graphics		X	X
Ultra-high-performance multicomputer for 3-D graphics		X	X
Haptic displays (force feedback for virtual environments)		X	X
Nanomanipulator		X	X
Optoelectronic head-tracker for head-mounted displays			X
Ultrasound visualization (augmented-reality echography display)		X	X
Electronic support measurement bistatic sensor technology		X	
Acoustic daylight ocean noise imaging system		X	
Laser beam propagation through atmospheric turbulence	X		
Integrated optical-digital correlation		X	
Real-time 3-D imaging and control		X	X
Directed search testbed and collaborative analysis and decision-making		X	X

D. TECHNOLOGY SURVEY FORMS

The remainder of this chapter is devoted to the presentation of the technology survey forms. In this initial phase, each technology is only briefly assessed on the form with respect to potential strengths, weaknesses, and operational applications. The great number of possible technologies, coupled with the complexities of obtaining detailed scientific knowledge argued for initially looking at a broad range of candidates to a purposely shallow depth.

The next phase of the task will select a small subset of these technologies and subject them to a more exacting assessment of feasibility and payoff potential. Those results will be reflected in parallel IDA Paper P-3157, *Information Warfare: Selected Long-Range Technology Applications*.

(This page is intentionally blank.)

CONCEPTS

Source: Institute for Defense Analyses

POCs: W. Barlow, (703) 845-2465
R. Turner, (703) 845-2434

TECHNOLOGY OVERVIEW

Description: Computing with DNA molecules

Who: Leonard M. Adleman, University of Southern California; Richard Lipton, Princeton University

Technology Strengths: Capability to execute NP-complete computations with simple protocols on DNA substrates; potential for information storage at a density of the order of 1 bit per cubic nanometer (b/nm^3); potential for executing computations at far higher rates that can currently be achieved in massively parallel supercomputers.

Technology Weaknesses: Approach does not provide flexibility that is inherent to electronic digital computers.

Dr. Adleman's approach applies to computational tasks that can be formulated as directed Hamiltonian path problems. Dr. Lipton is looking for methods that circumvent the task of formulating the problem as a Hamiltonian path.

Prototype Operational Concept(s): Massively parallel processor; high density information storage

Possible applications for high-density information storage.

Compatibility With Current Operating Environments: Unknown

Technological Risks: Possibility of errors in large-scale computations; real solutions may be lost in the procedure, and false solutions may be created.

Proprietary Aspects: Unknown

Patents, Patent Applications, Holders: Unknown

Potential Limiting Operational Parameters: Additional research is needed to attack problems involving large graphs.

Commercial Availability: None known

Source: Institute for Defense Analyses

POCs: W. Barlow, (703) 845-2465
R. Turner, (703) 845-2434

TECHNOLOGY OVERVIEW

Description: Stereo-image processing for active perception

Who: Computer Vision & Robotics Research Laboratory
Electrical & Computer Engineering Department
University of Tennessee
Knoxville, TN

Technology Strengths: Multiple application domains, automated reaction, and control potential

Technology Weaknesses: Computationally difficult problem(s), potentially compounded by real-time, environmental constraints

Prototype Operational Concept(s): Target-tracking algorithms
Spatio-temporal filters for motion perception
Image stream analysis for depth extraction
Automated recognition and control

Compatibility With Current Operating Environments: Should not be an issue.

Technological Risks: Unknown

Proprietary Aspects: Unknown

Patents, Patent Applications, Holders: Unknown

Potential Limiting Operational Parameters: Experimental technology

Commercial Availability: Unknown

Source: Institute for Defense Analyses

POCs: W. Barlow, (703) 845-2465
R. Turner, (703) 845-2434

TECHNOLOGY OVERVIEW

Description: Natural evolution of machine codes: digital organisms

Who: Thomas Ray (University of Delaware)
Dan Pirone (University of Washington)
Santa Fe Institute
Albuquerque, NM 87501

(Related research, on "evolutionary engineering," the creation and testing of very complex computers whose behavior cannot be predicted, is being performed by Dr. Hugo de Garis in Kyoto, Japan.)

Technology Strengths: Exploits evolution of mutatable self-replicating computer programs as a basis for achieving efficient parallel machine codes. Running the system under conditions that favor small, efficient algorithms has produced remarkable optimizations of machine code.

Technology Weaknesses: Further research is needed to obtain efficient codes to perform specified tasks.

Prototype Operational Concept(s): A new approach for generating software capable of fully exploiting the power of massively parallel computers.

Compatibility With Current Operating Environments: Unknown

Technological Risks: Unknown

Proprietary Aspects: Unknown

Patents, Patent Applications, Holders: Unknown

Potential Limiting Operational Parameters: Unknown

Commercial Availability: None known

Source: Institute for Defense Analyses

POCs: W. Barlow, (703) 845-2465
R. Turner, (703) 845-2434

TECHNOLOGY OVERVIEW

Description: Semiotics is a formal system of sign analysis that can be employed to study signs and symbols and their use in every aspect of a society's affairs.

Who: Dr. Daniel G.J. Chandler, University of Wales Aberystwyth, has made an excellent summary essay, "Semiotics for Beginners," available via the Internet. Early work was done by Charles S. Pierce (U.S.) and Ferdinand de Saussure (France). This work has been continued and elaborated by numerous academic researchers in the United States and abroad.

Related research may be underway at the Xerox Palo Alto Research Center.

Technology Strengths: Brings formal methods to bear on problems related to the transmission and strategic use of information via signs, symbols, and imagery.

Technology Weaknesses: Exploration of applications appears to be at a very preliminary stage.

Prototype Operational Concept(s): Substantial improvements in capabilities for processing, structuring, and transmitting information to enhance utility to information users and strengthen command decision-making.

Systematic approach for identifying and exploiting signs and symbols that are important to other societies and for structured development of offensive IW capabilities that rely on symbolism.

Compatibility with Current Operating Environments: No manifest incompatibilities with ongoing information system elements or research efforts (hardware, software, visualization, artificial intelligence).

Proprietary Aspects: Unknown

Patents, Patent Applications, Holders: Unknown

Potential Limiting Operational Parameters: Not applicable

Commercial Availability: None known

Source: Institute for Defense Analyses

POCs: W. Barlow, (703) 845-2465
R. Turner, (703) 845-2434

TECHNOLOGY OVERVIEW

Description: Mediology--a successor to semiotics

While the neurosciences are dedicated to overcoming the inherent duality between mind and brain, mediology tries to view history by hybridizing technology and culture. Debray believes that developers of semiotics have been overly focused on "the code" or symbols, while ignoring what they are "really used for in the milieu." He also asserts that many researchers have overemphasized the impact of information-related technologies without regard to a nation's social and cultural contexts.

Who: Regis Debray, French intellectual

Technology Strengths: Panoramic viewpoint for Information Warfare strategy

Technology Weaknesses: May be limited to development of general strategic or policy guidelines.

Prototype Operational Concept(s): Improved understanding of a given society through the lens of mediology can boost the efficiency of prewar and wartime Information Warfare (including psychological operations) as well as peacetime diplomacy.

Compatibility With Current Operating Environments: Debray's views are not widely recognized or understood.

Technological Risks: Unknown

Proprietary Aspects: Unknown

Patents, Patent Applications, Holders: Not applicable

Potential Limiting Operational Parameters: Not applicable

Commercial Availability: None known

Source: Institute for Defense Analyses

POCs: W. Barlow, (703) 845-2465
R. Turner, (703) 845-2434

TECHNOLOGY OVERVIEW

Description: Direct link from the brain to a computer

Concept is based on extended voluntary control of brain-wave pattern(s) similar to what has been accomplished through biofeedback training.

Who: Jonathan Wolpaw
Wadsworth Laboratories
New York State Department of Health

Work in this area is also being done by a team at Wright Patterson AFB.

Technology Strengths: Opens up possibility of completely new functional interfaces beyond what can be achieved with keyboards, other manual devices, and voice control.

Technology Weaknesses: Long-range research project; may not provide significant enhancements over current interfaces; policy implications are not well understood.

Prototype Operational Concept(s): Direct data transfer from the brain to the computer and communication through thoughts

Seamless control of piloted vehicles

Compatibility With Current Operating Environments: None

Technological Risks: Unknown

Proprietary Aspects: Unknown

Patents, Patent Applications, Holders: Unknown

Potential Limiting Operational Parameters: Differences in how similar thoughts are manifested in different individuals may impose fundamental constraints on the kinds of interactions that are feasible.

Commercial Availability: None known

Source: Institute for Defense Analyses

POC: Terry Mayfield, (703) 845-6602

TECHNOLOGY OVERVIEW

Description: Computational sociology

Worldwide interconnected computing has resulted in the formation of "computational societies" or "computational ecosystems" that collaborate and cooperate as well as compete for resources. The advent of distributed artificial intelligence (DAI) and agent-based software has evoked the need to treat their interactions as those of human-like "social creatures," who must provide for the common good (e.g., system efficiency) as well as carry out tasks that are specific to their individual interests. Behavioral conflicts will arise that result in system inefficiencies or localized operational failures. Certain behaviors (e.g., cascading failures, swarming) could lead to catastrophic failures. The focus here is to examine the algorithms used by these software agents and to rework them in such a way that inefficiency is reduced, failures are avoided, and globally optimum performance is achieved. Methods being examined to achieve appropriate behaviors include market-oriented programming (based on market price mechanisms), genetic algorithms, adaptation heuristics, negotiation protocols, contract protocols, and networking protocols with quality-of-service parameters. The specification of system operational concepts requires dealing with distributed system software entities (e.g., agents) and their interaction policies in the context of system-wide optimizations with respect to efficiency, protection, and reliability. Behavior and behavioral tradeoffs must be understood and appropriately controlled at both the local and global levels to achieve optimal results. Software and system behaviors equate to the interactions of the specified policies and policy goals.

Who: Xerox Palo Alto Research Center; IBM Research; Santa Fe Institute; SRI International; University of Michigan (Ann Arbor); University of Arizona; University of Massachusetts (Amherst); Cornell University; Internet (IETF); AT&T Bell Labs; Center for Coordination Science, MIT

Technology Strengths: Potential for more efficient and dynamically adaptable systems, leading to more robust systems to the extent that protection and reliable behavior are targeted.

Technology Weaknesses: Implementation of narrowly scoped protocols or algorithms that only emphasize efficiency can detract from achievement of protection and reliability enhancement attributes. Adding research on fault-tolerant and degraded operational behavior would strengthen this area significantly.

Prototype Operational Concept(s): Dynamically adaptable systems can extend the defensive capabilities of a computational infrastructure, which is key to defensive Information Warfare, especially in massively distributed processing systems.

Technological Risks: Unknown

Compatibility With Current Operating Environments: Should not be an issue apart from security reliability enhancement needs.

Proprietary Aspects: Unknown

Patents, Patent Applications, Holders: Unknown

Potential Limiting Operational Parameters: Scalability

Commercial Availability: Unknown

DEVICE TECHNOLOGIES

Source: Joint Staff (J6K)

POC: LTC Michael F. Napoliello, (703) 614-7813

TECHNOLOGY OVERVIEW

Description: Fiber Optic Undersea Information Network (AT&T SeaNet): a lightweight underwater fiber optic cable system with wet-mate couplers for rapid deployment. Cable engine does not require specialized vessels for cable laying. Provides the opportunity for high bandwidth communications across great distances using the advantages of fiber optic cable.

Who: Dr. Clark DeHaven, Jr., AT&T Bell Labs

Technology Strengths: Existing technology

Small, lightweight fiber optic cables, repeaters & multiplexers

Unmanned Undersea Vehicle (UUV) connectivity

Technology Weaknesses: Known weakness due to availability of means for penetration and compromise of fiber optic cables. However, this is mitigated by the hostile environment in which the cable is deployed.

Maximum operational depth unknown.

Prototype Operational Concept(s): Rapid response capability for Information & C2 Warfare

Unload MILSATCOM Networks

Global commercial fiber optic connectivity for joint warfare

Communications support to passive undersea surveillance arrays

Compatibility with Current Operational Environments: Can interface with available fiber-optic-based information technology.

Technology Risks: Initial deployment and maintenance costs

Proprietary Aspects: AT&T is the sole developer of the cable and wet-mate couplers.

Patents, Patent Applications, Holders: AT&T

Potential Limiting Operational Parameters: Determined by devices connected to the network.

Commercial Availability: Yes (through AT&T)

Source: Joint Staff (J6K)

POC: LTC Michael F. Napoliello, (703) 614-7813

TECHNOLOGY OVERVIEW

Description: Microelectromechanical Sensors. SARCOS has developed a suite of microelectronics sensors which contain the sensor and post-processor on the same silicon wafer base.

Who: SARCOS Research Corporation, Mr. Peter Kind, (801) 581-0155

Technology Strengths: Places sensor processor on the same silicon wafer as the sensor.

Reduces sensor bandwidth requirements.

Enables "Information Driven Machines that Move."

Technology Weaknesses: Current developments have focused on mechanical sensor types:

- Uni-axial strain transducer
- Rotary displacement transducer
- Multi-axial strain transducer
- Multiplexing
- Wobble motor.

Prototype Operational Concept(s): Near-real-time adaptive sensor arrays and control actuators

Compatibility with Current Operational Environments: Unknown

Technology Risks: Sensitivity to highly and vibration environments; residual vibration effects on sensor elements

Patents, Patent Applications, Holders: SARCOS

Potential Limiting Operational Parameters: Output torque/power; response time to transient imagery

Commercial Availability: SARCOS

Source: Institute for Defense Analyses

POCs: W. Barlow, (703) 845-2465
R. Turner, (703) 845-2434

TECHNOLOGY OVERVIEW

Description: Femtosecond laser pulses

Who: Professor Warren S. Warren, et al. (applications to molecular chemistry)
Department of Chemistry
Princeton University
Princeton, NJ 08544-1009

E. A. De Souza, M. C. Nuss, W. H. Knox and D. A. B. Miller (multiplexing)
AT&T Bell Laboratories

Howard Milchberg and Charles Durfee (plasma-guided beams, soft x-ray pulses)
University of Maryland

Technology Strengths: Shaping femtosecond (i.e., of the order of 10^{-15} second) laser pulses permits encoding 1 gigabit (Gb) (10^9 bits) per second information streams on a laser beam with a duty cycle of the order of 10^{-4}. Such beams can be multiplexed to achieve an overall transmission rate of the order of a terabit (10^{12} bits) per second.

Alternatively, a single transmission beam can be used to achieve extremely high immunity to jamming.

Technology Weaknesses: Laser links in the atmosphere can be degraded or interrupted by adverse weather conditions.

Prototype Operational Concept(s): Provide wideband relay of multiplexed near-real-time imagery data or other wideband phenomenology on satellite-to-satellite links or between satellites and high-flying aircraft.

Compatibility With Current Operating Environments: Some information sources capable of 1 Gbps rates exist.

Technological Risks: Technology is being developed as a tool for molecular chemistry research.

Proprietary Aspects: Unknown

Patents, Patent Applications, Holders: Unknown

Potential Limiting Operational Parameters: Relativistic effects, peak power limitations, need to convert information to longer wavelengths for transmission over long atmospheric paths.

Commercial Availability: None known

Source: Institute for Defense Analyses

POCs: W. Barlow, (703) 845-2465
R. Turner, (703) 845-2434

TECHNOLOGY OVERVIEW

Description: Electrooptical data storage on thin-film photoconductive materials.

Who: Chong-yang Liu, Horng-long Pan, Marye Anne Fox, and Allen J. Bard
Department of Chemistry and Biochemistry
University of Texas
Austin, TX 78712

Technology Strengths: Very high speed optical and electronic writing and reading of information on a thin-film photoconductor[1] at high spatial densities. Storage densities of 3 Gb/cm^2 with no cross-talk between adjacent memory elements have been demonstrated and higher densities should be possible. Measurements support the possibility of attaining subnanosecond read-write times.

In addition to conventional data storage applications, major conceptual advances in signal and image processing can be projected because of the possibilities of combining electronic and optically implemented functions.

Technology Weaknesses: Pending development of pulse sequence to integrate reading and rewrite functions, contents must be read and rewritten periodically, because readout process gradually diminishes quality/strength of recorded bits.

Prototype Operational Concept(s): DRAM for advanced imagery processing applications (e.g., synthetic aperture radar imaging of moving targets)

Electronic read mode for very high capacity ROM for storage of high-resolution graphical materials

Possible applications of optical read mode to optical signal processing, e.g., holography, high-speed optical correlators for automatic target recognition

Technological Risks: Unknown

Compatibility With Current Operating Environments: Should not be an issue.

Proprietary Aspects: Unknown

Patents, Patent Applications, Holders: Unknown

Potential Limiting Operational Parameters: The charge-trapping mechanism is not yet well understood. Demonstrated storage densities have been achieved using a scanning tunneling microscope. Storage density for optical write-read operations is limited by the size of the laser beam.

---

1 The material employed is a liquid crystal, zinc-octakis (β-decoxyethyl) porphyrin (ZnODEP), held between transparent indium-tin-oxide sheets.

Commercial Availability: The storage medium itself is simple and inexpensive. Effort has been supported by the Texas Advanced Technology Program.

Source: Institute for Defense Analyses

POCs: W. Barlow, (703) 845-2465
R. Turner, (703) 845-2434

TECHNOLOGY OVERVIEW

Description: Three-dimensional holographic storage of digital information

Who: John F. Heanue
Department of Applied Physics
Stanford University
Stanford, CA 94305-4090

Matthew C. Bashaw and Lambertus Hesselink
Department of Electrical Engineering
Stanford University
Stanford, CA 94305-4035

Demetri Psaltis and Allen Pu
California Institute of Technology
Pasadena, CA

Fai Mok	Kevin Curtis
Holoplex	AT&T
Pasadena, CA	Bell Labs

Technology Strengths: Storage densities of 3 x 10^9 pixels per cubic centimeter and transfer rates of $6x10^6$ bits per second have been demonstrated; goal is storage of terabytes of data, transfer rates >1 Gbps, random access time < 100 microseconds (μs).

Storage of information in holographic form offers important opportunities for new approaches to optical processing and information security.

Technology Weaknesses: Speed of recording holographic images is currently severely limited by the properties of the photorefractive material (lithium niobate).

Requires error correction coding to accommodate raw bit error rates (BERs) of 10^{-4} to 10^{-3} at higher storage densities. (Such error rates are of little significance for storage of uncompressed video.) Use of 12-bit Hamming error-correction coding and burst-error control procedures has demonstrated a BER of 10^{-6} in the prototype configuration.

Requires periodic rewrite because repeated read operations gradually erase the holographic images. A "fixing" process can be used for long-term storage, such as read-only memory (ROM) applications.

Prototype Operational Concept(s): Employs spatial light modulator to record spatially multiplexed holograms of "pages" of source material (e.g., 1 page per 50 microradians) in a photo refractive crystal. Readout employs CCD array; all elements (pixels) of a stored page are reconstructed simultaneously. Concept supports storage of very large quantities of high resolution color imagery, compressed and uncompressed video, and data.

Future possibility is for new approaches for cross-correlating imagery with stored references in support of automatic target classification or other pattern recognition applications.

Compatibility With Current Operating Environments: Has been used to store and retrieve a high-fidelity color image and a 10-frame video that had been stored in digital form in a conventional computer hard drive.

Technological Risks: Scalability

Proprietary Aspects: Unknown

Patents, Patent Applications, Holders: Unknown

Potential Limiting Operational Parameters: Attainable storage density is determined by BER requirements; page-to-page convolutional coding approaches should be examined.

Commercial Availability: None known

Source: Institute for Defense Analyses

POCs: W. Barlow, (703) 845-2465
R. Turner, (703) 845-2434

TECHNOLOGY OVERVIEW

Description: Passive millimeter-wave camera

Who: TRW Space and Electronics Group, EPI/ETA Technologies, University of California at Los Angeles, McDonnell Douglas Aerospace, Army Research Laboratory, Air Force Wright Laboratory, NASA Langley Research Center (consortium)

Technology Strengths: To provide TV-like images through fog, clouds, smoke, dust, and sandstorms.

Implementation is based on DoD-developed microwave/millimeter wave integrated circuit (MIMIC) components.

Technology Weaknesses: Wavelengths are much longer than is the case for electrooptical cameras, and resolution is poorer. Technology is still in research phase.

Prototype Operational Concept(s): All-weather vision systems for pilots

Surveillance and reconnaissance applications to detect and identify targets for advanced precision-guided weapons under adverse visibility conditions without requiring signal transmission

Possibly significant sensory advantage to combat personnel under adverse visibility conditions

Strong potential for a range of surveillance applications, e.g., for decoy discrimination

Compatibility With Current Operating Environments: Consistent with efforts to exploit active millimeter-wave technology

Technological Risks: Unknown

Proprietary Aspects: Unknown

Patents, Patent Applications, Holders: Unknown

Potential Limiting Operational Parameters: Limited range and resolution (depends on intrinsic target signature strength, size of antenna aperture and other factors); severely adverse weather will degrade performance.

Commercial Availability: Possible commercial applications

Source: Institute for Defense Analyses

POCs: W. Barlow, (703) 845-2465
R. Turner, (703) 845-2434

TECHNOLOGY OVERVIEW

Description: Cesium vapor optical correlator

Who: Ivan Biaggio, Jouni P. Partanen, B. Al, Randall J. Knize, and Robert W. Heilwarth
Departments of Electrical Engineering and Physics
University of Southern California
Los Angeles, CA 90089-0484

Technology Strengths: Use of cesium vapor as the nonlinear optical comparison medium yields high sensitivity, high resolution, very high speed (30 ns comparison response time has been demonstrated), with low-power operation.

Technology Weaknesses: Under study

Prototype Operational Concept(s): Video image pattern recognition or comparison at perhaps 1,000 frames per second, to be used for processing reconnaissance imagery, weapon guidance, quality control (e.g., inspection of items produced in very large quantities).

Compatibility With Current Operating Environments: Physical setup is simple. CCD array of a commercial video camera can be used to detect and display the two-dimensional cross-correlation function of the input and reference images.

Technological Risks: Unknown

Proprietary Aspects: Unknown

Patents, Patent Applications, Holders: Unknown

Potential Limiting Operational Parameters: Image processing capacity is presently limited by existing spatial light modulators and output analyzers. Spatial light modulators that can display and erase 256x256 pixel images in 100 μs have been reported, which is about 300 times slower than the intrinsic rate that the correlator is capable of achieving.

Commercial Availability: None known

Source: Institute for Defense Analyses

POCs: W. Barlow, (703) 845-2465
R. Turner, (703) 845-2434

TECHNOLOGY OVERVIEW

Description: Blue-green diode lasers

Who: Gertrude Neumark, Henry Krumb School of Mines, Columbia University
Robert Park, University of Florida in Gainesville
James DePuydt, 3M Photonics Technology Laboratory, Saint Paul, MN

H. Morkoç and S. N. Mohammad
Materials Research Laboratory
Coordinated Science Laboratory
University of Illinois at Urbana
Urbana, IL 61801

Technology Strengths: Compact, reliable, inexpensive source of short wavelength laser radiation.

Shorter wavelength permits smaller spot size for optical recording and playback and thereby permits increased recording density and higher data transfer rates.

Technology Weaknesses: Short operating lifetime

Prototype Operational Concept(s): Applications for high-resolution optical recording; possible sensor and communications applications

Compatibility With Current Operating Environments: Should not be an issue.

Technological Risks: Unknown

Proprietary Aspects: Unknown

Patents, Patent Applications, Holders: Unknown

Potential Limiting Operational Parameters: Under study

Commercial Availability: There is extensive foreign interest in short wavelength diode lasers.

Source: Institute for Defense Analyses

POCs: W. Barlow, (703) 845-2465
R. Turner, (703) 845-2434

TECHNOLOGY OVERVIEW

Description: Gallium nitride blue and ultraviolet laser diodes

Who: Cree Research, Inc., and Philips Laboratories - Briarcliff (a division of Philips Electronics North America)

First successful gallium nitride LED (January 1993) has been attributed to Shuji Nakamura, Nichia Chemical, Shikoku, Japan

Technology Strengths: Combines the robust properties of gallium nitride thin films with realization of GaN light-emitting diodes on silicon carbide wafers. Earlier work based on zinc selenide technology was less efficient and required cryogenic cooling.

Technology Weaknesses: Unknown

Prototype Operational Concept(s): High density optical data storage, e.g., multi-gigabyte optical disks to replace CD-ROMs; lightweight countermeasure systems; covert communications; chemical-biological reagent detection

Compatibility With Current Operating Environments: Should not be an issue.

Technological Risks: Unknown

Proprietary Aspects: Unknown

Patents, Patent Applications, Holders: Unknown

Potential Limiting Operational Parameters: Unknown

Commercial Availability: None known

Source: Institute for Defense Analyses

POCs: W. Barlow, (703) 845-2465
R. Turner, (703) 845-2434

TECHNOLOGY OVERVIEW

Description: Protein-based computers

Who: Robert R. Birge
W. M. Keck Center for Molecular for Molecular Electronics and NY State Center for Advanced Technology in Computer Applications and Software Engineering
Syracuse University
Syracuse, NY 13210

Technology Strengths: Highly compact, high-performance data storage and processing capabilities are potentially available through laser excitation of protein (e.g., bacteriorhodopsin) molecules, with the potential of a 50-fold size reduction.

Technology Weaknesses: Early research phase; prototype parallel-processing devices, three-dimensional data storage hardware, and neural networks have been constructed.

Prototype Operational Concept(s): Associative memories, parallel processing architectures, three-dimensional memories, neural networks, holographic applications.

Compatibility With Current Operating Environments: Unknown

Technological Risks: Unknown

Proprietary Aspects: Unknown

Patents, Patent Applications, Holders: Unknown

Potential Limiting Operational Parameters: Thermal environment constraints

Commercial Availability: Worldwide interest

Source: Institute for Defense Analyses

POCs: W. Barlow, (703) 845-2465
R. Turner, (703) 845-2434

TECHNOLOGY OVERVIEW

Description: Optical flux-monitoring molecular beam epitaxy control system

Who: Kevin Killeen
Chemical Science Processing Department
Sandia National Laboratories
Albuquerque, NM

Technology Strengths: Real-time control of growth rates to <1 percent facilitates precision growth of electronic and optical devices. Distributed Bragg reflectors consisting of 12 periods of aluminum arsenide and gallium arsenide have been grown with thicknesses of 70 and 83 nm, respectively, with thickness accuracy of the order of 0.2 nm (0.3 percent).

Technology Weaknesses: Growth rate achieved in the laboratory prototype is about 0.3 nm/s. Work is under way to extend the technique to indium devices; ability to employ other materials in this approach to precise molecular beam epitaxy has not yet been demonstrated.

Prototype Operational Concept(s): Production of sensor components by molecular beam epitaxy. Production of vertical cavity surface emitting lasers to replace semiconductor lasers.

Compatibility With Current Operating Environments: Concept is designed to be compatible with existing molecular beam epitaxy machines.

Technological Risks: Unknown

Proprietary Aspects: Unknown

Patents, Patent Applications, Holders: Unknown

Potential Limiting Operational Parameters: Accuracy of the epitaxial growth process is determined by capability to stabilize the intensity of the light beam used to monitor the deposition process.

Commercial Availability: This effort is one being undertaken by a partnership between universities, industry, and the Government, including the Universities of New Mexico, Southern California, and Virginia; Chorus Corporation/EPI Division, Hughes, Superior Vacuum Technology, Texas Instruments, and J.A. Woolan Company; and ARPA.

Source: Institute for Defense Analyses

POCs: W. Barlow, (703) 845-2465
R. Turner, (703) 845-2434

TECHNOLOGY OVERVIEW

Description: Quantum electronic computer device technology

Includes enhanced conventional devices such as high electron mobility transistors and fundamentally new approaches, such as storing data in the electronic energy levels of an atom.

Who: AT&T Bell Labs, Motorola

In Japan: Basic Research Laboratories, Nippon Telegraph and Telephone; Quantum Electron Devices Laboratory, Fujitsu; Hitachi, Matsushita; Mitsubishi; NEC; Sony; Sumitomo Electric; Toshiba

Seth Lloyd
Department of Mechanical Engineering
MIT, Cambridge, MA, 02139

D. Deutsch, A. Barenco, & A. Ekert
(quantum cryptography)
Oxford University
Oxford, England

R. Josza
University of Plymouth
Plymouth, England

Tycho Sleator
New York University
New York, New York

Harald Weinfurter
University of Innsbruck
Innsbruck, Austria

Use of ions as computational elements:
Peter Zoller and J. I. Cirac
University of Innsbruck
Innsbruck, Austria

Technology Strengths: Concepts envision exploiting quantum mechanical effects to achieve reduced size, increased speed, better energy efficiency of computer logical elements, relative to contemporary semiconductor devices.

Technology Weaknesses: Technologies are still very much in the research phase. Issues to be resolved include application concepts for basic phenomena, mechanisms for storage and retrieval, and operating temperature (cryogenic versus uncooled). Longer-term approaches will almost certainly require new logical concepts.

Prototype Operational Concept(s): Miniaturized computer logic with greatly increased speed, computing power.

Compatibility With Current Operating Environments: None

<u>Technological Risks</u>: Unknown

<u>Proprietary Aspects</u>: Unknown

<u>Patents, Patent Applications, Holders</u>: Unknown

<u>Potential Limiting Operational Parameters</u>: Possible sensitivity to external electromagnetic fields

<u>Commercial Availability</u>: None

Source: Institute for Defense Analyses

POCs: W. Barlow, (703) 845-2465
R. Turner, (703) 845-2434

TECHNOLOGY OVERVIEW

Description: Modulatable retroreflectors for coherent CO_2 laser communication

Who: Gregory Olson, Hans W. Mocker, Nick A. Demma, and Jamie Billing Ross
Honeywell Technology Center, Honeywell Inc.
3660 Technology Drive
Minneapolis, MN 55418

Technology Strengths: Voice-modulated corner reflector illuminated by a highly directional CO_2 laser provides a reliable, high-quality voice communication link between a transmit-receive station and a remotely located unit, facility, or individual. Transmit-receive station can determine the location of the remote unit.

Equipment size and power minimum requirements at the remote location are minimum; retroflector area is 5 cm^2, modulation power requirement is <10 mW (watch-type battery is used in the prototype).

Atmospheric range of 24 km has been demonstrated with a 10-watt laser; potential range is 250 km if the transmit-receive station is airborne.

Technology Weaknesses: Requires line-of-sight path; range is reduced by atmospheric effects (dense fog).

Prototype Operational Concept(s): Tower-mounted, balloon-borne, or helicopter-borne transmit-receive station provides secure, low-probability-of-intercept, jam-resistant, tactical communications with long-range patrols and special operations forces; maintains precise knowledge of location and status of unit.

Compatibility With Current Operating Environments: Represents a wholly new architectural approach to tactical communications.

Technological Risks: Signal acquisition procedures, frequency stability.

Proprietary Aspects: Unknown; prototype design contains several unique features.

Patents, Patent Applications, Holders: Unknown

Potential Limiting Operational Parameters: Range is generally limited by atmospheric transmission parameters. Higher data rates can be achieved at the expense of complexity of the remote unit.

Commercial Availability: None known; possible application to area control of robotic devices.

Source: Institute for Defense Analyses

POCs: W. Barlow, (703) 845-2465
R. Turner, (703) 845-2434

TECHNOLOGY OVERVIEW

Description: Holographic visor displays

Who: Y. Amitai, S. Reinhorn, and A. A. Freeman
Department of Physics of Complex Systems
Weizmann Institute of Science
Rehovot 76111 Israel

Technology Strengths: Design method for compact holographic doublet visor displays, capable of providing excellent (essentially diffraction-limited) imaging performance, relatively low chromatic dispersion over a wide field of view (± 6° has been demonstrated).

Avoids need for computer-generated holograms, aspherical lenses.

Technology Weaknesses: Early in the development cycle

Prototype Operational Concept(s): Visor displays for command-and-control and information analysis applications

Heads-up displays for vehicles and aircraft

Compatibility With Current Operating Environments: Extends applications of holographic visor displays to nonmonochromatic light sources, e.g., cathode ray tubes.

Technological Risks: Performance in combat vibration environment.

Proprietary Aspects: Unknown

Patents, Patent Applications, Holders: Unknown

Potential Limiting Operational Parameters: Unknown

Commercial Availability: None known

Source: Institute for Defense Analyses

POCs: W. Barlow, (703) 845-2465
R. Turner, (703) 845-2434

TECHNOLOGY OVERVIEW

Description: Integrated neural network for image detection and classification

Who: Richard G. Stearns
Xerox Palo Alto Research Center
3333 Coyte Hill Road
Palo Alto, CA 94304

Technology Strengths: Capability to sense and classify optical images at video rates

Liquid crystal display can be employed as a programmable filter for image processing

Technology Weaknesses: Requires training

Prototype Operational Concept(s): Automatic classification of reconnaissance imagery

High-speed automatic character recognition for hand-lettered text

Compatibility With Current Operating Environments: Compact configuration, great potential for scalability

Technological Risks: Requirement for training quality optical reference materials

Proprietary Aspects: Unknown

Patents, Patent Applications, Holders: Unknown

Potential Limiting Operational Parameters: Error rate depends on extent of training, size of reference image set

Commercial Availability: None known

SOFTWARE

Source: Joint Staff (J6K)

POC: LTC Michael F. Napoliello, (703) 614-7813

TECHNOLOGY OVERVIEW

Description: Real-time video insertion. Technology to intercept, in real-time, a video stream and to insert images not originally in the video.

Who: National Information Display Laboratory: Stephanie Baldwin, (609) 734-2737

Technology Strengths: Real time video processing

Can be PC driven
Seamless insertion.

Technology Weaknesses: Requires prescreening.

Prototype Operational Concept(s): Extract critical image elements from irrelevant background.

Superimpose prerecorded video imaging on real-time video broadcasts.

Compatibility with Current Operational Environments: Compatible with most known video formats

Technology Risks: Susceptibility to video editing (e.g., same-day tapes); applicability to novel television signal formats, e.g., high-definition TV and highly compressed video.

Proprietary Aspects: NIDL Proprietary

Patents, Patent Applications, Holders: NIDL

Potential Limiting Operational Parameters: Under study

Commercial Availability: The technology is being marketed commercially by NIDL for selective advertising during telecasts of sporting events.

Source: Joint Staff (J6K)

POC: LTC Michael F. Napoliello, (703) 614-7813

TECHNOLOGY OVERVIEW

Description: Fractal Information Storage

Who: Cross/Z International, Inc., Joseph Furnia

Technology Strengths: Automatic data encryption as part of the data base design

Prevents user direct access to source records
Massive data compression
Ideal structure for data mining and decision support environments
Data is unintelligible without access to generation infrastructure.

Technology Weaknesses: Best utilized for very large size data bases

Possible loss of detail in fractal generation.

Prototype Operational Concept(s): High volume data base designs based on transposition to a mathematical fractal base. Data retrieval utilizes fractal segment matching.

Compatibility with Current Operational Environments: Fractal data bases can be generated from most available data base management systems.

Technology Risks: Embryonic technology effort with limited commercial applications at this time.

Proprietary Aspects: Cross/Z International, Inc.

Patents, Patent Applications, Holders: Cross/Z International, Inc., on fractal generation algorithms

Potential Limiting Operational Parameters: Unknown

Commercial Availability: Cross/Z International, Inc.

Source: Institute for Defense Analyses

POCs: W. Barlow, (703) 845-2465
R. Turner, (703) 845-2434

TECHNOLOGY OVERVIEW

Description: Speech recognition technology (developing speech recognition capabilities for future DSPs in hand-held computers)

Who: (ARPA/TRP sponsored)
Dragon Systems (speech recognition business)
Analog Devices (signal processing business)

Technology Strengths: Objective is to replace keyboards on hand-held computers.

Technology Weaknesses: Technology in this area is not mature. Stress modifications to voice, voice recording, and playback are known weaknesses.

Prototype Operational Concept(s): Potential improvements in utility of portable computers to function in severe operating environments. The voice recognition system will replace tiny keyboards on hand-held computers that are difficult to use. The projected device will be able to cope with both small specialized technical vocabularies and large vocabularies for general dictation in real time. The speech recognition software will be scaleable to fit the memory available and thus be adaptable to multiple machines. May provide alternatives to conventional password techniques for user identification and authentication.

May eventually provide alternatives to conventional password techniques for user identification, authentication.

Compatibility With Current Operating Environments: Little compatibility with current environments

Technological Risks: Unknown

Proprietary Aspects: ARPA sponsored; project will most likely will produce a research prototype that will be developed by participants commercially.

Patents, Patent Applications, Holders: Unknown

Potential Limiting Operational Parameters: May be susceptible to failure in environments that are speech "unfriendly," e.g., high-noise background.

Commercial Availability: Not currently available as a robust technology. Somewhat available in low functionality, high-error rate form.

Source: Institute for Defense Analyses

POCs: W. Barlow, (703) 845-2465
R. Turner, (703) 845-2434

TECHNOLOGY OVERVIEW

Description: Distributed execution environment for high-performance parallel processing

Who: Partha Dasgupta, Arizona State University; Zvi Kedem, New York University

Technology Strengths: Integrates three paradigms developed in theoretical research:

- Eager scheduling ensures that all "free" workstations participate in the computation in a wait-free-like manner. This allows available workstations to overtake more loaded or failed ones at a cost of some replication of the computational tasks.
- Evasive memory layouts decouple memory addressing from logical memory storage, preventing slow or late processors from clobbering data.
- Dispersed data management provides fault tolerance in memory at a lower cost than conventional replication.

These approaches enable a computing platform consisting of a network of workstations with distributed memory to execute applications with high performance and fault tolerance, while avoiding costly mechanisms such as distributed synchronization, coherence, replication, and global scheduling.

Technology Weaknesses: Unknown

Prototype Operational Concept(s): Permits practical design of a computing platform based on off-the-shelf workstations that achieves the power, reliability, and programming convenience of supercomputers.

Compatibility With Current Operating Environments: Should not be an issue.

Technological Risks: Unknown

Proprietary Aspects: Unknown

Patents, Patent Applications, Holders: Unknown

Potential Limiting Operational Parameters: Depends on aggregate workstation and interconnection capacity

Commercial Availability: None known

Source: Institute for Defense Analyses

POCs: W. Barlow, (703) 845-2465
R. Turner, (703) 845-2434

TECHNOLOGY OVERVIEW

Description: Image deblurring

Who: Alfred S. Carasso
Computing and Applied Mathematics Laboratory
National Institute of Standards and Technology
Gaithersburg, MD

Technology Strengths: This mathematical approach is deterministic and does not require *a priori* assumptions about the character of the data noise or the nature of the ideal image. In particular, it relaxes smoothness constraints required by many image deblurring procedures but is highly effective in suppressing noise. (Enforced smoothness constraints may be dangerous in some imaging contexts where unsuspected singularities may be present in the ideal image.)

Technology Weaknesses: Unknown

Prototype Operational Concept(s): Improved image quality for reconnaissance, surveillance, and other imaging processes (e.g., astronomy and ultrasound imaging)

Compatibility With Current Operating Environments: Should not be an issue.

Technological Risks: Impact on image interpretation capabilities has not been determined.

Proprietary Aspects: Unknown

Patents, Patent Applications, Holders: Unknown

Potential Limiting Operational Parameters: May not be suitable for compressed imagery.

Commercial Availability: None known

Source: Institute for Defense Analyses

POCs: W. Barlow, (703) 845-2465
R. Turner, (703) 845-2434

TECHNOLOGY OVERVIEW

Description: Multispectral imagery analysis

Who: Stephen J. Ford and David M. McKeown
Computer Science Department
Carnegie-Mellon University
Pittsburgh, PA 15213

Technology Strengths: Produces a synthetic, three-dimensional image dataset using surface material information fused with estimates of height based upon stereo matching in high-resolution panchromatic imagery. Provides basis for evaluation of methods to generate and validate a ground-truth, surface material map, using available information and remotely sensed data.

Technology Weaknesses: Unknown

Prototype Operational Concept(s): Potential new capabilities for near-real-time access of reconnaissance imagery, e.g., for bomb damage assessment

Compatibility With Current Operating Environments: Should not be an issue.

Technological Risks: Unknown

Proprietary Aspects: Unknown

Patents, Patent Applications, Holders: Unknown

Potential Limiting Operational Parameters: Experimental technology

Commercial Availability: None known

Source: Institute for Defense Analyses

POCs: W. Barlow, (703) 845-2465
R. Turner, (703) 845-2434

TECHNOLOGY OVERVIEW

Description: Speech recognition for Windows-equipped personal computers

Who: Microsoft Research Speech Technology Group (Windows-equipped PCs)
Microsoft Corporation, Advanced Technology Division
3635 157th Avenue, Building 11
Redmond, WA 98052

James K. Baker (multilingual capabilities for PCs and workstations)
Dragon Systems, Inc.
320 Nevada Street,
Newton, MA 02160 (617) 965-5200

In addition, natural language speech recognition work is being done by InfoSeek of Santa Clara, CA. IBM is marketing speech recognition features in commercial equipment.

Technology Strengths: Advanced speech recognition features on a low-cost, highly available platform. Integrated speech recognition and input capability for personal computers using Microsoft Windows. Improved efficiency, usability, and accuracy. Provides continuous speech recognition, user independence, online

Source: Institute for Defense Analyses

POCs: W. Barlow, (703) 845-2465
R. Turner, (703) 845-2434

TECHNOLOGY OVERVIEW

Description: Softcopy mapping system (SMS) for data fusion and mapping applications

Who: Lockheed Missiles and Space Company, Inc.
SMS Support
Lockheed Austin Division
P.O. Box 17100
Austin, TX 78760-7100

Technology Strengths: Displays map data from multiple sources after they have been preprocessed into a common format by the SMS tool. Equips system developers with tools to integrate SMS into their applications. Provides a portable software environment for exploiting high performance graphic environments.

Technology Weaknesses: Unknown

Prototype Operational Concept(s): Provides a large range of map-based interactive display capabilities.

Compatibility With Current Operating Environments: Designed to be flexible, portable, and easy to use. Sources include Defense Mapping Agency, United States Geological Survey, and United States Census Bureau.

Technological Risks: Intrinsic interoperability problem of disparate graphics standards

Proprietary Aspects: Unknown, but most likely any rights are held either by Lockheed or (possibly) contracting organization.

Patents, Patent Applications, Holders: Unknown

Potential Limiting Operational Parameters: May not be suitable for inputs in compressed formats.

Commercial Availability: Yes

Source: Institute for Defense Analyses

POCs: W. Barlow, (703) 845-2465
R. Turner, (703) 845-2434

TECHNOLOGY OVERVIEW

Description: Neural networks and fuzzy logic

Who: Bart Kosko (fuzzy logic)
Signal and Image Processing Institute
University of Southern California
Los Angeles CA 90007

BrainTech (neural networks and fuzzy logic)
Scottsdale, AZ

Technology Strengths: Circumvents the need to identify specific features, logical weights, and decision criteria for specific sorting tasks involving complex data or imagery.

Technology Weaknesses: Cause-and-effect relationships that endow these approaches with decision-making attributes are generally unknown.

Prototype Operational Concept(s): Automatic target recognition in reconnaissance imagery

Processor for hand-written text; information security tool for authenticating personal signatures of various types

Automatic control of vehicles; weapon control and guidance

Remote diagnosis of an individual's health

Compatibility With Current Operating Environments: Should not be an issue.

Technological Risks: Possibility of failing to treat new inputs as unrecognizable

Proprietary Aspects: Unknown

Patents, Patent Applications, Holders: Unknown

Potential Limiting Operational Parameters: Capability to discriminate between similar inputs

Commercial Availability: None known

Source: Institute for Defense Analyses

POC: Ron Ross, (703) 845-6617

TECHNOLOGY OVERVIEW

Description: Security architectures: the DoD Goal Security Architecture (DGSA)

Separation technology: hardware, firmware, and software that enforces strict isolation between multiple information domains across a distributed network of end systems.

Security management technology: automated and administrative tools for managing the creation, use, and maintenance of information domains within a distributed network.

Security protocol technology: elements required to provide a secure transfer system for passing information from an information domain across a network.

Who: NSA, DISA, NIST

Technology Strengths: Excellent architectural principles and concepts; natural methodology for organizing and separating critical information essential for enterprise operations.

Technology Weaknesses: Separation technologies, while fundamentally sound, will be difficult to implement on a commercial scale.

Prototype Operational Concepts: Security products and mechanisms that can be used by system architects, engineers, and integrators to build information systems meeting mission-oriented security requirements.

Compatibility With Current Operating Environments: Current mainstream commercial, operating systems do not provide necessary features to support the DGSA and the information domain construct. The DGSA will rely on next-generation separation technologies using microkernel-based operating systems and memory management facilities employing 64-bit addressing.

Technological Risks: Commercial viability, attainability of DGSA objectives

Proprietary Aspects: Some separation technology, security management technology, and security protocols technology will be proprietary.

Patents, Patent Applications, Holders: Not applicable

Potential Limiting Operational Parameters: Not applicable

Commercial Availability: Limited

Source: Institute for Defense Analyses

POCs: Terry Mayfield, (703) 845-6602

TECHNOLOGY OVERVIEW

Description: Distributed operating systems for increased real-time, reliable performance to support multimedia applications.

Who: University of Washington, Carnegie-Mellon University, OSF Research Foundation, Sun Microsystems, Microsoft, Taligent, University of Utah, MIT, University of Arizona

Technology Strengths: Evolution of the technology is supported by a diverse and robust research community and is influenced by more powerful addressing schemes (64-bit single-space addressing, virtual addressing); object-oriented technologies; new service paradigms such as object brokering; advent of agent-oriented software and distributed artificial intelligence programs; nomadic computing; closer coupling of networking protocols with operating system microkernels.

Technology Weaknesses: Increased complexity, issues pertaining to scalability, lack of information protection functionality. Complexity can be reduced by modularity, generally with a performance penalty. Scalability entails operating system components that can manage very large heterogeneous distributed systems. Information protection features entail performance penalties, costs to the vendor for providing assurances that protection functionality is adequate, and cryptographic features.

Prototype Operational Concepts: Distributed operating systems will be object-based, task-oriented, protocol-driven, and directory-supported. Task-oriented, adaptable agents will enhance nomadic computing, electronic commerce, rapid and interoperable configuration of heterogeneous components, and information discovery. Protection will come from strong encapsulation with domain and type enforcement and negotiated security protocols.

Compatibility With Current Operating Environments: Most distributed operating systems being fielded will have the capability to interact with fielded computing systems, using present file-exchange procedures. Cryptography issues may cause interoperability problems.

Technological Risks: Major risk is capability to incorporate cryptographic functionality. The issue of "trust" associated with cryptographic certification is paramount and must be resolved consistently with international interoperability and security policies of participating nations.

Proprietary Aspects: Most vendor-supplied software will be proprietary. Some cryptographic features will be proprietary; other cryptographic features will be restricted due to national security constraints.

Patents, Patent Applications, Holders: Cryptography patents are held by RSA, Inc., and Public Key Partners.

Potential Limiting Operational Parameters: Cryptographic features, scalability

Commercial Availability: Distributed operating system software is just beginning to enter the commercial market. Most of this software is based on a client-server model, and systems using a broker style of computing are being implemented, e.g., Taligent, OMG CORBA.

Source: Institute for Defense Analyses

POCs: Terry Mayfield, (703) 845-6602

TECHNOLOGY OVERVIEW

Description: Distributed multimedia processing

Distributed multimedia applications will be the technology driver for computing and communications over the next decade.

- Networking infrastructure: increased bandwidth and reliable service for high-speed communications
- Workstations: reliable, real-time processing
- Operating systems: fundamental changes to accommodate low latency, continuous-media processing, e.g., audio and video streams, and asynchronous video-on-demand requirements.

Processing model will be based on adaptive resource management with deterministic execution. ATM networking technology, rate-based execution (RBE) schedulers, quality-of-service guarantees, and high-speed, agile encryptors will provide the base to meet processing requirements.

Who: ARPA, NSA, MCNC, University of North Carolina at Chapel Hill, Hybrid Networks, Stanford University, AT&T Bell Labs, MIT, ATM Forum, et al.

Technology Strengths: Furthers the modes of human-computer interaction, enabling real-time video conferencing, collaborative work flow, compound documents, new spatial and temporal analysis tools, and virtual reality.

Technology Weaknesses: Synthesis of supporting technologies to enable distributed multimedia processing is still in the research phase; security issues have not been addressed. Research is needed on protection of media forms and service points; security policy and policy enforcement implementation are important in this regard.

Prototype Operational Concept(s): Real-time teleconferencing for large-scale collaborative planning, command and control, and other applications

Integration and analysis of intelligence, reconnaissance, surveillance, and force status information for real-time, synoptic situational awareness

Psychological operations; perception management

Compatibility With Current Operating Environments: Not fully compatible with the current operating environment; issues are sufficient bandwidth, capability to process continuous media with real-time guarantees to attain appropriate fidelity and reliability.

Technological Risks: The synthesized technology has not been operationally tested sufficiently, and many rough spots, e.g., faults and unpredictable performance characteristics, may appear. Operational feedback will be needed to improve component technologies as well as the synthesized technology. Resolution of the aforementioned protection issues may determine the extent to which distributed multimedia processing becomes operationally significant.

Proprietary Aspects: Most components of the synthesized technology are proprietary.

Patents, Patent Applications, Holders: Unknown

Potential Limiting Operational Parameters: Performance may be constrained by security assurance overhead.

Commercial Availability: Commercial efforts, e.g., Hybrid Networks, are underway; many components are commercially available.

Source: Institute for Defense Analyses

POC: Terry Mayfield, (703) 845-6602

TECHNOLOGY OVERVIEW

Description: Agent-oriented software/distributed artificial intelligence

Development and use of software components that act on behalf of another agent (e.g., a human user) or interact among themselves as cooperating or competing agents to perform specifically tailored or heuristically determined tasks. Such agents may be fixed, declarative, or procedural programs (e.g., scripts), or small, adaptable, distributed artificial intelligence systems (e.g., expert systems).

Who: ARPA; Stanford University; University of Massachusetts; Xerox Palo Alto Research Center; Dr. Pattie Maes, Media Lab, MIT; Santa Fe Institute; Sloan School of Management, MIT.

Technology Strengths: Potential for substantially enhanced responsiveness to heterogeneity, task tailoring, dynamic adaptability, autonomy, intelligence, and cooperative operation. This emerging technology will significantly change the nature of our computing and communications infrastructure, i.e., operating systems networking, database management systems, human/computer interactions, systems management, and user applications.

Technology Weaknesses: Roles and implications of agent-oriented software/distributed artificial intelligence remain to be fully explored. Issues of policy and management with respect to individual and multi-agent ethics and behaviors (e.g., collaboration, cooperation, competition, negotiation, and protection) have not been adequately addressed. The policy area of protection is only now beginning to emerge in the research field; issues of identification and authentication, authorization, delegation, negotiation, and encapsulation are critically important. Role-based security policies and domain-type enforcement will be needed.

Prototype Operational Concept(s): Task-oriented, adaptable agents to extend the capabilities of human and machine resources, by enhancing capabilities for nomadic computing, electronic commerce, rapid and interoperable configuration of heterogeneous system components, and information discovery. Such agents could also support a new paradigm for information security.

Compatibility With Current Operating Environments: Agent-oriented software has been developed for a number of systems and applications, e.g., MIME messages, WWW Spiders and Robots, Macintosh Assistants.

Proprietary Aspects: Some agent-oriented software is proprietary.

Technological Risks: No mechanisms such as encapsulation have incorporated in currently fielded systems to confine the behavior of agent-oriented systems; this allows insertion of Trojan Horse code into the agent-receiving (client) systems with full client privileges.

Patents, Patent Applications, Holders: Unknown

Potential Limiting Operational Parameters: Security assurance measures may limit functionality.

Commercial Availability: Agent-oriented software and tools, e.g., General Magic's Telescript and Macintosh Assistants, are commercially available; however, much of the commercially available software is embedded in commercial applications or systems.

Source: Institute for Defense Analyses

POCs: W. Barlow, (703) 845-2465
R. Turner, (703) 845-2434

TECHNOLOGY OVERVIEW

Description: Network Intrusion Detection

Who: Computer Operations, Audit, and Security Technology (COAST) Project
Computer Science Department
Purdue University
Lafayette, IN 47907

Technology Strengths: Employs two approaches for detecting intrusions: detection of security-relevant events, and tracking user behavior to detect anomalies.

Technology Weaknesses: Can miss real intrusions and generate false indications of intrusions. Not all security-relevant events can be known beforehand; user behavior can be mimicked, and the intrusion detection mechanism can be conditioned.

Prototype Operational Concept: Embedded audit system within a network or distributed system generates event records that are sent to one or more reconciliation mechanisms. Selected event types (e.g., link failure) are flagged and administrators are alerted automatically. User behavior is recorded in profiles that are compared with current activity, so that deviations from experienced behavior are detected and reported.

Compatibility With Current Operating Environments: Compatible with some current operating environments

Technological Risks: Another challenge to the hackers' community

Proprietary Aspects: Unknown

Patents, Patent Applications, Holders: Unknown

Potential Limiting Operational Parameters: Event record generation, collection, and processing are overhead operations from the standpoint of primary functionality.

Commercial Availability: Some commercial products are available.

Source: Institute for Defense Analyses

POCs: W. Barlow, (703) 845-2465
R. Turner, (703) 845-2434

TECHNOLOGY OVERVIEW

Description: Collaborative information sharing on the World Wide Web

Who: Computer Science and Artificial Intelligence Laboratory
MIT, Cambridge, MA

In conjunction with the World Wide Web (W3) Consortium

Technology Strengths: Capability to provide distributed "groupware" applications. State-of-the-art information sharing tools that can be applied in a variety of Information Warfare domains.

Technology Weaknesses: Requires secure distributed infrastructure and communications.

Prototype Operational Concept(s): The intelligence community has recognized the value of an Internet-like infrastructure and has implemented a secure version (Intelink) of the Internet set of protocols. Distributed groupware will support important applications for intelligence and other defense communities.

Compatibility With Current Operating Environments: Highly compatible

Technological Risks: Vulnerability to virus insertion

Proprietary Aspects: Unknown

Patents, Patent Applications, Holders: Unknown

Potential Limiting Operational Parameters: Security must be provided in a distributed environment.

Commercial Availability: None known

Source: Institute for Defense Analyses

POCs: W. Barlow, (703) 845-2465
R. Turner, (703) 845-2434

TECHNOLOGY OVERVIEW

Description: Wavelet-based image compression

Who: Victor Korsun
National Information Display Laboratory
David Sarnoff Research Center
Princeton, NJ 08543-8619

Charles K. Chui and P. K. Yuen
Houston Advanced Research Center
The Woodlands, TX

Technology Strengths: Integrates a number of software features to achieve up to 300:1 compression in the number of bits required to represent color photographs, maps, and other graphical materials; this represents a 15-fold improvement over standard image compression techniques.

Enables rapid transmission of such materials at bit rates, e.g., 14.4 kbps, employed by Internet modems. Substantially reduces storage requirements.

Algorithms can exploit full capacity of the transmission path; facilitates use of intermittently available communication links for transfer of imagery data.

User can select small areas of special interest for transmission without loss of image quality.

Technology Weaknesses: Vulnerability to interference

Prototype Operational Concept(s): Situational awareness information, e.g., from airborne surveillance and reconnaissance systems, would be integrated to provide a common situational picture that could be quickly distributed and frequently updated. The wavelet-based image compression technique would be incorporated in tactical communications to geographically distributed units equipped with laptop computers. This capability would facilitate rapid forward-area interpretation and feedback of situational awareness information; encourage prompt feedback on maneuver and strike options; and could substantially reduce risks of fratricide, entrapment by enemy forces on the move.

Compatibility With Current Operating Environments: Well-matched to the desk-top or laptop computer environment. Software algorithms and available transmission rates support full-motion video on 486-class machines.

Proprietary Aspects: Unknown

Patents, Patent Applications, Holders: Unknown

Potential Limiting Operational Parameters: May not support transmission of analytical quality imagery without interpretive operator interaction to select compression ratio, e.g., 100:1 instead of 300:1, or areas of special interest.

Commercial Availability: Available

SYSTEMS INTEGRATION

Source: Joint Staff (J6K)

POC: LTC Michael F. Napoliello, (703) 614-7813

TECHNOLOGY OVERVIEW

Description: Three-dimensional Command-and-Control Information Display

Who: Stephanie Baldwin, (609) 734-2737
National Information Display Laboratory (NIDL)
David Sarnoff Research Center
Princeton, NJ 08543

Technology Strengths: High data representation

Greater perceptual addressibility
Fewer image controls

Technology Weaknesses: Dependence on high-definition TV technology

Control based on speech recognition technology

Prototype Operational concept(s): Improved man-machine interface at command nodes, for better situation awareness

Interactive command decision making.

Compatibility with Current Operational Environments: Can be used with existing tactical data links after data formats have been programmed into the fusion application.

Technology Risks: Risks appear to be mainly associated with development of reliable voice control technology.

Proprietary Aspects: NIDL

Patents, Patent Applications, Holders: NIDL

Potential Limiting Operational Parameters: Human capacity to assimilate and interact

Commercial Availability: Pending (NIDL)

Source: Institute for Defense Analyses

POCs: W. Barlow, (703) 845-2465
R. Turner, (703) 845-2434

TECHNOLOGY OVERVIEW

Description: Synchronous Optical Network (SONET)

Who: AT&T Bell Labs; Southwestern Bell, Inc.; AT&T Bell Laboratories; Rockwell International Corporation; Tektronix, Inc.; and Washington University (St. Louis)

Technology Strengths: An experimental SONET fiber-optic network and asynchronous transmission mode (ATM) self-healing ring, with potential for achievement of a survivable, very high capacity fiber-optic information distribution network. Implemented with low-level communications technology, allowing higher-level services (e.g., multimedia) to use high bandwidth.

Technology Weaknesses: Unknown

Prototype Operational Concept(s): Target system will be an OC-192 (10 Gbps) self-healing fiber optic transmission system. The proposed system promises reductions in network complexity and cost, increases in network efficiency, and high-capacity data throughput. A self-healing ring network can survive network node failures or optical fiber cuts, permitting computer networks to automatically operate around a failed network node.

Compatibility With Current Operating Environments: Requires extensive fiber-optic infrastructure. Use of ATM facilitates multimedia applications (data, digital voice, digital video and imagery) and enhances utility for a wide range of military users.

Technological Risks: Unknown

Proprietary Aspects: SONET is an open standard (produced by BellCoRe).

Patents, Patent Applications, Holders: Unknown

Potential Limiting Operational Parameters: Probably requires fixed backbone (i.e., non-mobile technology)

Commercial Availability: This technology is claimed to be critical to developing the National Information Infrastructure. Several SONET products are available (e.g., from WilTel Network Services and Integrated Telecom Technology), but their use for this application is unknown. It is likely that project will yield a research prototype product, which project members will try to commercialize.

Source: Institute for Defense Analyses

POCs: W. Barlow, (703) 845-2465
R. Turner, (703) 845-2434

TECHNOLOGY OVERVIEW

Description: Wearable computer systems with transparent, headmounted displays

Who: (ARPA TRP): Boeing Computer Services; Honeywell Military Avionics Division; Virtual Vision, Inc.; Carnegie Mellon University

Technology Strengths: Successful development could enhance information connectivity and weapon control flexibility to combat personnel, battle staff.

Technology Weaknesses: Limited set of application areas for the immediate future

Prototype Operational Concept(s): Computer with transparent, head-mounted display and position-sensing system interface. One version of the system will superimpose images directly on the surface of objects, and a second version will project text and images onto the operator's protective face shield. This will enable "hands-free" presentation of information for manufacturing, assembly, maintenance, or training operations to improve productivity and accuracy. This effort will combine commercial virtual reality technology with Department of Defense-developed components.

Compatibility With Current Operating Environments: Currently little compatibility with current environments

Technological Risks: Unknown

Proprietary Aspects: Supported by ARPA; prototype likely to be developed commercially by participants.

Patents, Patent Applications, Holders: Unknown

Potential Limiting Operational Parameters: User is head-encumbered. This may not be a drawback if technology can be integrated with existing use of headgear.

Commercial Availability: Little to no availability

Source: Institute for Defense Analyses

POCs: W. Barlow, (703) 845-2465
R. Turner, (703) 845-2434

TECHNOLOGY OVERVIEW

Description: 3-D micro-imaging and visualization of fluid transport processes in micro-electromechanical systems

Who: Anne-Marie Lanzillotto, Mike Amabile, Tzong-Shyng Leu, Mike Sawicki, and Rick Wildes
David Sarnoff Research Center
Princeton, NJ 08543-5300

John Dunsmuir
Exxon Research and Eng. Co.
Route 22 East
Annandale, NJ 08801

Technology Strengths: Integrates synchrotron x-ray source, high-speed CCD camera for x-ray microtomography, computer vision technology, and an image-processing supercomputer, to achieve high resolution (<3 micrometers), real-time, three-dimensional imaging of the internal microstructure and microdynamics of fluid displacement in microchannels and microvalves.

Permits determination of fluid displacement patterns and flow velocities.

Technology Weaknesses: Requires substantial investments in technologically complex equipment.

Prototype Operational Concept(s): Design tool for fluidic computers

Compatibility With Current Operating Environments: Should not be an issue.

Technological Risks: Unknown

Proprietary Aspects: Unknown

Patents, Patent Applications, Holders: Unknown

Potential Limiting Operational Parameters: Turbulent flow

Commercial Availability: None known

Source: Institute for Defense Analyses

POCs: W. Barlow, (703) 845-2465
R. Turner, (703) 845-2434

TECHNOLOGY OVERVIEW

Description: High-performance multicomputer for 3-D graphics

Who: Henry Fuchs and John Poulton
Department of Computer Science
University of North Carolina at Chapel Hill

Technology Strengths: This system, named Pixel-Planes 5, has demonstrated a capability to produce textured polygons at rate of 2.3×10^6 triangles per second (terrain fly-through application).

Uses custom-designed computer chips that integrate processor and memory functions.

Renders images with advanced lighting models (including specular highlights and multiple light sources) and textures.

Ring network operates at an aggregate data rate of 160 million 32-bit words per second (8 simultaneous data streams of 20 million 32-bit words per second).

Technology Weaknesses: Requires substantial investment in what is currently custom-fabricated computer hardware.

Prototype Operational Concept(s): Modular array of Graphics Processors connected to an array of Renderers by a Ring Network, which also drives the Frame Buffer that assembles the full-screen image. Applications include high-fidelity simulation for training and tactics development; command displays for enhanced situation awareness and options assessment.

Compatibility With Current Operating Environments: Several layers of software support are provided to handle needs ranging from application programming to algorithm developers. Programming tools and graphics libraries allow applications developed in C to utilize nearly the full performance of the machine. Existing applications that use the PHIGS+ standard for 3-D graphics can readily be ported to the system.

Technological Risks: Unknown

Proprietary Aspects: Unknown

Patents, Patent Applications, Holders: United States Patents 4,590,465 (basic architecture) and 4,783,649 (renderer implementation)

Potential Limiting Operational Parameters: Overall size limited to 3 card cages, each with 18 slots for application boards

Commercial Availability: Sponsored by ARPA and NSF, with significant additional assistance from Digital Equipment Corporation, Hewlett-Packard, and Intel.

Licenses have been granted to Division Ltd., a manufacturer of turnkey virtual reality systems, and IVEX, Inc., maker of image generators for flight simulation and training.

Source: Institute for Defense Analyses

POCs: W. Barlow, (703) 845-2465
R. Turner, (703) 845-2434

TECHNOLOGY OVERVIEW

Description: Ultra-high-performance multicomputer for 3-D graphics

Who: Henry Fuchs and John Poulton
Department of Computer Science
University of North Carolina at Chapel Hill

Technology Strengths: This system, named Pixel Flow, is projected to exceed 10 million textured polygons per second, or more than four times the graphics generation speed of Pixel Planes 5.

Technology Weaknesses: Leading edge technology

Prototype Operational Concept(s): High-fidelity interactive real-time display of situational awareness information

Compatibility With Current Operating Environments: Programming tools and graphics libraries allow applications developed in C to utilize nearly the full performance of the machine. Existing applications that use the PHIGS+ standard for 3-D graphics can readily be ported to the system. Applications include high-fidelity simulation for training and tactics development; command displays for enhanced situation awareness and options assessment.

Technological Risks: Unknown

Proprietary Aspects: Unknown

Patents, Patent Applications, Holders: Unknown

Potential Limiting Operational Parameters: Compressibility of products for telecommunications

Commercial Availability: Sponsored by ARPA and NSF, with significant additional assistance from Division Group PLC and Hewlett-Packard. Licenses have been granted to Division Ltd., a manufacturer of turnkey virtual reality systems, and IVEX, Inc., maker of image generators for flight simulation and training.

Source: Institute for Defense Analyses

POCs: W. Barlow, (703) 845-2465
R. Turner, (703) 845-2434

TECHNOLOGY OVERVIEW

Description: Haptic displays--force feedback for virtual environments

Who: Fred Brooks
Department of Computer Science
University of North Carolina at Chapel Hill
Chapel Hill, NC

Technology Strengths: Gives the user the ability to feel objects or force fields in a virtual environment. Can improve interactive task performance significantly, e.g., 30 percent improvement in performing a complex 6-D docking task relative to a visual-only display.

Technology Weaknesses: Interaction volume is limited by available manipulators.

Prototype Operational Concept(s): Remote weapon and platform control applications; assembly and repair functions involving manipulation of objects on the nanometer scale; enhanced situation awareness for command displays when integrated with high-performance graphics multicomputer arrays.

Compatibility With Current Operating Environments: System is well documented. Advanced force-feedback software library with Application Programmer Interface has been developed and supports distributed operation. Supports the Argonne Remote Manipulator (6° of freedom), the Sarcos arm (10° of freedom) and the Phantom arm (will be upgraded for 6° of sensing and 4° of actuation). Additional devices can be supported by writing device-driver software; software library automatically scales positions and forces.

Technological Risks: Unknown

Proprietary Aspects: Source code and documentation for the software library are available.

Patents, Patent Applications, Holders: Unknown

Potential Limiting Operational Parameters: Limited scope of man-machine interactions imposed by manipulator technology

Commercial Availability: Sponsored by NIH National Center for Research Resources, ARPA, and NSF/ARPA Science and Technology Center for Computer Graphics and Scientific Visualization, with significant additional assistance from Silicon Graphics Corporation and Hewlett-Packard

Source: Institute for Defense Analyses

POCs: W. Barlow, (703) 845-2465
R. Turner, (703) 845-2434

TECHNOLOGY OVERVIEW

Description: Nanomanipulator

Who: Frederick P. Brooks, William V. Wright,
Russell Taylor, and Vernon L. Chi
Department of Computer Science
University of North Carolina at Chapel Hill

Richard Superfine and Sean Washburn
Department of Physics & Astronomy
University of North Carolina at Chapel Hill

Stan Williams, University of California at Los Angeles

Technology Strengths: Provides an intuitive interface to scanning probe microscopes, permitting the operator to manipulate nanometer-scale structures. Presents a three-dimensional image in real-time and force-feedback control.

Technology Weaknesses: Current configuration is a research tool.

Prototype Operational Concept(s): Assembly and repair functions involving manipulation of objects on the nanometer scale

Compatibility With Current Operating Environments--Proprietary Aspects: Should not be an issue.

Technological Risks: Unknown

Patents, Patent Applications, Holders: Unknown

Potential Limiting Operational Parameters: Speed of manipulation is limited.

Commercial Availability: Supported by NSF and NIH

Source: Institute for Defense Analyses

POCs: W. Barlow, (703) 845-2465
R. Turner, (703) 845-2434

TECHNOLOGY OVERVIEW

Description: Optoelectronic head-tracker for head-mounted displays

Who: Henry Fuchs (tracking) and Frederick P. Brooks, Jr. (architectural walk through)
Department of Computer Science
University of North Carolina at Chapel Hill

Technology Strengths: Provides tracking throughout an entire room with position accuracy better than 2 mm and orientation accuracy better than 0.1°. Tracker area of operation can be expanded without limit and avoids long-range distortions that affect magnetic tracking systems due to metal objects in the environment.

Approach is scaleable; update rate is typically >80 Hz; typical head-location measurement lag is 15 to 30 μs.

Supports see-through head-mounted "augmented reality" displays, which superimpose virtual images on the real-world environment. Augmented reality imposes much more stringent requirements on head-tracking accuracy than virtual environment applications.

Head-mounted display uses a stereo pair of high-contrast, frame-sequential, full color miniature CRT displays. Flicker is nonexistent because screens are updated at 180 times per second (60 times per second per color). Contrast ratio and resolution are each 10 times better than previous LCD displays.

Technology Weaknesses: Incorporation of hybrid inertial measurement techniques would aid delay-compensation routines and increase the restricted head rotation range of the current system.

Prototype Operational Concept(s): Employs a calibrated grid of infrared light-emitting diodes installed in the facility ceiling to provide position-fixing and angular references to optical sensors (lateral-effect diodes) on the head-mounted display. Computer determines the position and orientation of the operator's head by a photogrammetric technique known as space-resection by collinearity.

Compatibility With Current Operating Environments: Should not be an issue.

Technological Risks: Unknown

Proprietary Aspects: Unknown

Patents, Patent Applications, Holders: Unknown

Potential Limiting Operational Parameters: Limited volume over which tracking function can be implemented.

Commercial Availability: Sponsored by ARPA/ESTO, and NSF/ARPA Science and Technology Center for Computer Graphics and Scientific Visualization, with significant additional assistance from Digital Equipment Corporation and Hewlett-Packard.

Source: Institute for Defense Analyses

POCs: W. Barlow, (703) 845-2465
R. Turner, (703) 845-2434

TECHNOLOGY OVERVIEW

Description: Ultrasound visualization--augmented-reality echography display

Who: Henry Fuchs, Stephen M. Pizer, and Andrei State
Department of Computer Science
University of North Carolina at Chapel Hill

Technology Strengths: Integrates ultrasound imaging technology with a high-performance Silicon graphics Onyx Reality Engine^2 workstation and a head-mounted display equipped with a miniature video camera. Operator sees a real-time three-dimensional ultrasound image integrated with the camera image.

Technology Weaknesses: Algorithmic development required to improve performance, e.g., to eliminate spatial misregistration and perceived lag.

Prototype Operational Concept(s): Nonintrusive inspection, e.g., for concealed objects.

Compatibility With Current Operating Environments: Equipment complexity will limit applications.

Technological Risks: Capability to examine acoustically hard regions

Proprietary Aspects: Unknown

Patents, Patent Applications, Holders: Unknown

Potential Limiting Operational Parameters: Image quality and image generation speed are currently limited by the ultrasound machine. Ultrasound slice size (1 to 2 cm) degrades resolution in the direction perpendicular to the slice; efforts are under way to obtain access to thin-slice machines such as are used for cardiological examinations.

Commercial Availability: Significant assistance to the project has been provided by GE Medical Systems, PIE Medical Equipment, and Silicon Graphics Computer Systems.

Source: Institute for Defense Analyses

POCs: W. Barlow, (703) 845-2465
R. Turner, (703) 845-2434

TECHNOLOGY OVERVIEW

Description: Electronic support measurement bistatic sensor technology

Who: Rome Lab, Griffiss AFB, NY 13441-4514

Technology Strengths: Passive sensor system, using existing sources of illumination for ground-based or airborne surveillance.

Environmentally safe--requires no additional electromagnetic emissions to operate.

Technology Weaknesses: Unknown

Prototype Operational Concept(s): Covert tactical surveillance in a battlefield environment

Surveillance in support of counternarcotics, air traffic control, airport ground traffic control, and harbor traffic control operations

Compatibility With Current Operating Environments: Should not be an issue.

Technological Risks: Minimal, but internetting architecture may require further definition.

Proprietary Aspects: Unknown

Patents, Patent Applications, Holders: Unknown

Potential Limiting Operational Parameters: Coverage is determined by availability of electromagnetic emitters. Poor altitude accuracy in airspace surveillance applications.

Commercial Availability: None known

Source: Institute for Defense Analyses

POCs: W. Barlow, (703) 845-2465
R. Turner, (703) 845-2434

TECHNOLOGY OVERVIEW

Description: Acoustic daylight ocean noise imaging system (ADONIS)

Who: John R. Potter
Scripps Institution of Oceanography
La Jolla, CA

Technology Strengths: Employs naturally occurring random noise in underwater environments to create images of silent underwater objects; has produced images of moving targets in San Diego Bay.

Technology Weaknesses: Prototype has limited range; may require extensive arrays of elements.

Prototype Operational Concept(s): Mine countermeasures; submarine detection, classification

Compatibility With Current Operating Environments: Should not be an issue; may provide a useful complement to other surveillance capabilities

Technological Risks: May require extensive arrays of directional hydrophases and a dedicated communications network (e.g., AT&T SeaNet).

Proprietary Aspects: Unknown

Patents, Patent Applications, Holders: Unknown

Potential Limiting Operational Parameters: Array coverage; utility for deep ocean applications

Commercial Availability: None known

Source: Institute for Defense Analyses

POCs: W. Barlow, (703) 845-2465
R. Turner, (703) 845-2434

TECHNOLOGY OVERVIEW

Description: Laser propagation through atmospheric turbulence

Who: V. S. Rao Gudimetla and J. Fred Holmes
Oregon Graduate Institute of Science and Technology
20000 N.W. Walker Road
P.O. Box 91000
Portland, Oregon 97291-1000

Technology Strengths: Theoretical and experimental work intended to overcome a fundamental problem of using lasers as communication links, i.e., the attenuation of the received signal due to atmospheric effects. Uses multiple laser sources spanning the spectral region from blue to mid-infrared.

Technology Weaknesses: Primarily a research tool

Prototype Operational Concept(s): Potential for extending range, channel capacity of highly directional transmissions that are survivable and resistant to jamming and mutual interference.

Potential for long-range imaging applications.

Compatibility With Current Operating Environments: Will require new receiving, processing approaches for full exploitation.

Technological Risks: Unknown

Proprietary Aspects: Unknown

Patents, Patent Applications, Holders: Unknown

Potential Limiting Operational Parameters: Experimental technology

Commercial Availability: Unknown

Source: Institute for Defense Analyses

POCs: W. Barlow, (703) 845-2465
R. Turner, (703) 845-2434

TECHNOLOGY OVERVIEW

Description: Integrated optical-digital correlation

Combines the advantages of optical (for computationally intensive tasks) and digital processing (for filter selection and correlation analysis) to achieve a pattern or target recognition capability

Who: James P. Karins
Litton Data Systems (818) 706-4495 jkarins@vines.dsd.litton.com
Burbank, CA

Technology Strengths: Use of optical processing permits real-time exploitation of infrared, ladar, or electro-optical imagery in a compact configuration.

Technology Weaknesses: Typical data sources for optical correlation are susceptible to degradation in adverse weather.

Some applications require means for generating reference images that must meet similarity criteria.

Prototype Operational Concept(s): Precision weapon guidance

- Target identification
- Identification of friends
- Battle damage assessment

Compatibility With Current Operating Environments: Digital processor is open system, off-the-shelf; design is compatible with existing systems.

Technological Risks: Unknown

Proprietary Aspects: System is proprietary.

Patents, Patent Applications, Holders: Unknown

Potential Limiting Operational Parameters: Critical lens alignment tolerances for optical processing

Limited capability to ruggedize components for applications in stressed environments without affecting size and weight

Commercial Availability: Being marketed

Source: Institute for Defense Analyses

POCs: W. Barlow, (703) 845-2465
R. Turner, (703) 845-2434

TECHNOLOGY OVERVIEW

Description: Real-time 3-D imaging and control

Who: Multidimensional Applications and Gigabit Internetwork Consortium (MAGIC)
SRI International

Technology Strengths: Will enable a user to navigate in real time through a 3-D graphic representation of a real landscape created from elevation data and aerial images of that landscape. Real-time feeds of vehicle positions from portable GPS receivers can be superimposed on the display.

Technology Weaknesses: Requires high-bandwidth communications and massive processing capabilities.

Prototype Operational Concept(s): User remotely pilots a vehicle with a near-real-time, high-fidelity 3-D representation of the region. Locations of friendly forces and other important entities (e.g., radar emitters) can be incorporated in the visualization.

Compatibility With Current Operating Environments: Unknown

Technological Risks: Unknown

Proprietary Aspects: Funded by ARPA and NSF

Patents, Patent Applications, Holders: Unknown

Potential Limiting Operational Parameters: A failure in the supporting environment can cause failure of the entire system.

Commercial Availability: None known

Source: Institute for Defense Analyses

POCs: W. Barlow, (703) 845-2465
R. Turner, (703) 845-2434

TECHNOLOGY OVERVIEW

Description: Directed search testbed

Who: Mark Lister
National Information Display Laboratory
David Sarnoff Research Center
P.O. Box 8619
Princeton, NJ 08543-8619
(609) 951-0150

Technology Strengths: Enhanced capabilities to search softcopy intelligence materials for targets and activity indicators, based on exploitation of very-high-resolution display technology, improved head-mounted displays, collaborative environments.

Technology Weaknesses: Testbed activity is aimed at needs identification, supporting experimental assessments of emerging technology.

Prototype Operational Concept(s): Near-real-time analysis of reconnaissance imagery and other intelligence inputs, involving geographically separated teams and topical experts; immediate consensus as a basis for decision-making and identification of points of uncertainty as a basis for tasking of follow-up collection activities.

Compatibility With Current Operating Environments: Full exploitation of this concept may place considerable stress on capabilities to transmit and display high-resolution, high dynamic range imagery products.

Technological Risks: Means for incorporating heterogeneous intelligence materials in the search and analytical processes are still in the embryonic stage, but use of collaborative approaches may provide real insights into viable mechanisms for integrating multiple-source/multiple-phenomenology products.

Proprietary Aspects: Intelligence community sponsorship; significant commercial product potential, e.g., for analysis of medical imagery.

Patents, Patent Applications, Holders: Unknown

Potential Limiting Operational Parameters: Protocols for collaborational interactions; personnel training for interdisciplinary collaborational analysis and decision-making.

Commercial Availability: Silicon Graphics and others have an interest in the testbed project.

III. ACTIVITIES OF SELECTED DEFENSE AGENCIES RELEVANT TO INFORMATION WARFARE TECHNOLOGY

A. BACKGROUND

As noted in Chapter I of this document, the sponsors directed that the initial phase of the task be focused on technologies in the academic and private sectors. That desired concentration is represented in the technologies highlighted in Chapter II. During the data search phase of the survey, however, it became obvious that information on research and technology programs underway or planned by DoD and Government organizations was readily available. Inasmuch as a long-term goal of the Joint Staff effort is to develop a broad technology baseline that includes both DoD and private sector inputs, the IDA team elected to retain the material for future evaluation and potential inclusion in the emerging baseline. Examples of the relevant technologies and areas of interest are highlighted in this chapter.

Three defense agencies are directly involved in pursuit of information warfare technologies having substantial emphasis on defensive information warfare or information security activities. They are the Defense Information Systems Agency (DISA), the National Security Agency (NSA), and the Advanced Research Projects Agency (ARPA). A fourth agency, the Defense Airborne Reconnaissance Office (DARO) has prepared an airborne reconnaissance technology program plan to provide a systematic and comprehensive approach to developing supporting technologies for airframe, sensor information processing, and communications for many long-term, warfighting objectives relevant to information warfare.

B. DISA[1]

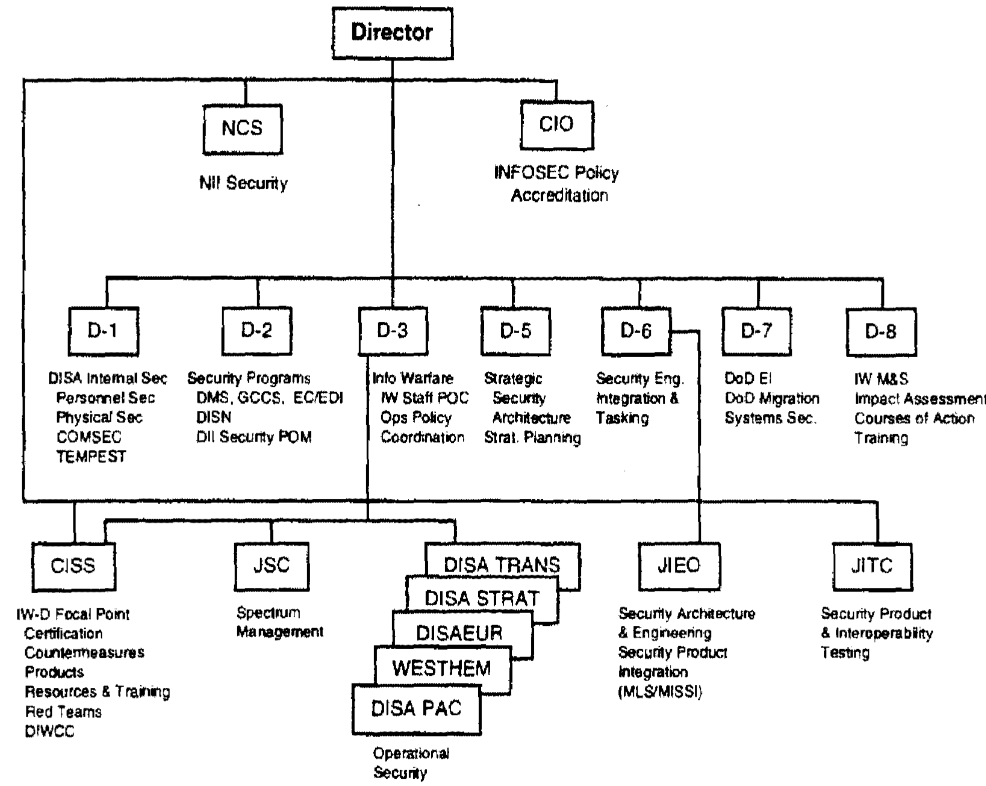
1. Overview

DISA plays a central role in the defensive IW effort, with the mission "to plan, engineer, develop, test, manage programs, acquire, implement, operate, and maintain information systems for C4I and mission support under all conditions of peace and war." DISA is the central manager of major portions of the Defense Information Infrastructure (DII) and acts as a customer to NSA and ARPA, implementing new technology and facilitating technology insertion into defense programs and systems. DISA is involved in the developing of information systems standards, developing information systems architectures, and performing assessments of existing systems; these efforts provide the frameworks and cohesion needed to bring technology to bear in meeting information security needs.

Of particular relevance is the responsibility assigned to DISA by DoD Directive 8000.1 that states that: "DISA, in collaboration with others, will assume the integrity of the Defense Information Infrastructure (DII) from exploration, corruption, or loss of science at an affordable cost."

To accomplish this task, DISA has organizationally allocated its Defensive Information Warfare (IW-D) functions as shown in Figure 2.

1 Material in this section is drawn from DISA Publication, *Defending the Defense Information Infrastructure (DII): DISA's Vision and Strategy for Defensive Information Warfare (IW-D)*, produced by the Center for Information Systems Security, September 1995.



Key

CIO:	Chief Information Officer
CISS:	Center for Information Systems Security
DII:	Defense Information Infrastructure
DISA:	Defense Information Systems Agency
DIWCC:	Defensive Information Warfare Control Center
DMS:	Defense Message System
EI:	Enterprise Integration
GCCS:	Global Command & Control System
IW:	Information Warfare
JIEO:	Joint Interoperability and Engineering Organization
JITC:	Joint Interoperability Test Center
JSC:	Joint Spectrum Center
M&S	Modeling & Simulation
MISSI:	Multilevel Information Systems Security Initiative
MLS:	Multilevel Security
NCS:	National Communication System

Figure 2. INFOSEC IW-D Structure in DISA

As seen in Figure 2, DISA IW-D functions are spread across many different organizations; however, the DISA Deputy Directorate for Operations (D3) is the focal point for all DISA IW activities. The operational focal point for defensive information warfare in DISA is the Center for Information Systems Security (CISS), which is under the operational oversight of D3. DISA and NSA established CISS to coordinate and execute the defense of the DII and to implement the Defense Information Systems Security Program (DISSP). While IW-D and security are everyone's business, CISS serves as the overall point of contact in DoD and DISA for implementing the defense of the information systems and data. CISS is responsible for DII certification and accreditation, the Department of Defense Information Systems Security Incident Response, vulnerability analysis, the mitigation strategies. CISS also provides information systems security training course and curriculum development, centralized information systems security Services contract management, the development and maintenance of a coordinated information systems security products database, and other related Services. The CISS program is jointly manned and executed by DISA and NSA.

2. Example Technology Research Areas

In the area of IW research and development (R&D), DISA, NSA, ARPA have signed a memorandum of agreement (MOA) to cooperate in the development of new IW security tools and applications. ARPA will bring its ability to apply high risk R&D to solve complex problems requiring advanced technology. They also support state-of-the-art feasibility demonstrations using leading edge technology. NSA brings the expertise in cryptology development and encryption along with much experience in conducting vulnerability analysis for the intelligence community. DISA will provide the testbeds for inserting these new technologies into information systems operations in a scaleable, modular fashion and will support the transition of the prototypes into production systems that can support the entire DII. The Services also bring extensive expertise with their Service laboratories and C^4I development centers for taking new developments supporting IW-D and tailoring them to support the tactical environments and Service-unique mission applications. DISA will also work closely with other Federal agencies such as the Department of Energy and their national labs, the Department of Commerce with its National Institute for Standards & Technology (NIST), and the Departments of Treasury and Justice.

Two important areas of cooperation between DISA and NSA are the Multilevel Security (MLS) initiative and the Multilevel Information Systems Security Initiative (MISSI). A variety of security products being developed under NSA's MISSI will be employed in each of the core DII programs. Commercial-off-the-shelf security products will also be used where they complement or enhance MISSI product capabilities. DISA and NSA have been working in coordination with the Joint Staff, the Military Services, Defense and Intelligence Agencies, to integrate these MISSI and commercial-off-the-shelf products into each of the core DII programs. The fiscal year 1996 defense budget includes funding to implement the Defense Message System (DMS) and procure security hardware and software for DMS, Defense Information System Network (DISN), and the Defense Megacenters (DMCs). MISSI is evolving a series of products that combine to provide security Services for a wide variety of application environments. These products include the following:

a. In-Line Network Encryptors (INE)

These products typically reside at the boundary between local and wide area networks and provide highly robust encryption and access control Services. *Fastlane* is a prime example of an INE.

b. Workstation Products

These products reside at individual workstations and provide writer-to-reader security Services. MISSI workstation products include the *Fortezza*-protected workstations and the Workstation Security Package (WSP).

c. Firewalls and Secure Server Products

A *Firewall* is a set of components used to control access between two networks. The Server products typically reside on the local net to provide common security Services for a variety of applications. An example is the Secure Network Server (SNS) functioning as a Security Policy Enforcement tool at the border. An SNS can also act as a secure fire server inside the border.

d. Network Security Managers

These encompass such security measures as cryptographic keying, access control, authentication, and use of passwords. Within MISSI, these Services, which are essential to most MISSI products, include the following:

- Certificate Authority Workstations (CAW), formerly known as Local Authority Workstations (LAW), typically reside on the local system and provide security support for the provision of capabilities such as digital signatures, cryptographic key, and access control permissions.
- Rekey Manager--Works in conjunction with Electronic Key Management System to provide cryptographic rekey support for MISSI products.

- Audit Manager--When completed in 1997, this product will provide support for the collection and analysis of security-relevant auditable events associated with MISSI products. An example of an auditable event is a repeated failed user login.
- X.500 Directory--Essential for providing global E-mail addressing, the directory provides a repository for public security information essential for MISSI product operation. An example is the public part of a users' digital signature.

e. Multilevel Security (MLS)

The goal of MLS is to allow systems of different overall classification levels to exchange information at a common level. This requires protective measures to ensure that no unauthorized information is released from the higher classified system to the lower system and that the lower system does not have unauthorized access to the other system. The DoD MLS office in DISA JIEO is responsible for managing the overall MLS program and in getting MLS products that are available today out to the field. NSA under their MISSI program is working towards long-term development efforts to solve the overall MLS goal of seamless interoperability between systems of different classification.

C. NSA

1. Overview

At NSA, defensive information warfare technology research is an important emerging component of the mission of the R2 organization.[2] Table 8 lists areas of activities of NSA/R2 in Information Security and indicates responsibilities in the related areas of high performance computing and communications.

---

2 This information is based on a briefing by [redacted] (b)(3):50 USC §402 Note of NSA/R2 to the JWCA IW Technology Subgroup on June 21, 1995.

Table 8. NSA/R2 Information Systems Security Program (ISSP)

Function	Responsible Office
• Formal Methods	R2 SPO
• ISSP-Cryptomath - CCR Math Increment - SCC Effort on Locked Workstations - Algorithm Development	R21
• ISSP-Engineering - Communication System Technology (Speech Processing and Wireless) - Cryptologic Design Technology (High Speed Electronics, Integrated Optics, Programmable Crypto, Fail-Safe Design	R-22
• ISSP-Computer Science - Information Security Assurance (Methods, Countermeasures, University Research) - Multilevel secure networked distributed systems (high speed, secure interoperability, data base management)	R23
The information set forth in Table 8 represents the status of the functions shown that existed in mid-1995. Because of the dynamic nature of Defensive Information Warfare, a number of changes have taken place since then, especially in the area of intrusion detection and response. Therefore, the information in this table should be viewed as work in progress and by no means represents all the activity relevant to the current status.	

2. Example Technology Research Areas

a. Trusted Operating Systems

- Commercial off-the-shelf (COTS)
- Incorporate high assurance methods and use basic building blocks
- Protection for crypto
- Eliminate costly components.

b. Firewalls

- Integrate strong cryptography
- Continuous authentication
- Multi-zone protection.

c. Network Countermeasures

- Novell Security Studies
- [redacted] (b)(3):50 USC §402 Note
- Firewall protection for selected systems.

d. Security Management

- Toolset for configuration and management of local/network security.

e. High-Speed Crypto

- High-speed electronics
- Synchronous Optical Network (SONET)
- Asynchronous Transfer Mode (ATM)
- Integrated optics.

f. Biometrics

- Voice
- Fingerprint
- Retinal
- Attack resistance.

g. Cryptography

- Fast encryption algorithms
- Quantum cryptography
- Adaptable cryptography.

h. Databases

- Multi-label data
- Distributed heterogeneous, interoperable
- Multi-media
- Object-oriented, real time.

D. ARPA

1. Overview

ARPA activities in developing IW technology are extensive. Table 9 indicates that before August 8, 1995, several offices were supporting projects relevant to IW technology. A large number of these projects were clustered in the ARPA Computing Systems Technology Office (CSTO).

Table 9. Overview of ARPA Information Warfare Activities

ADVANCED SYSTEMS TECHNOLOGY OFFICE (ASTO) Research Areas	COMPUTING SYSTEMS TECHNOLOGY OFFICE (CSTO) Research Areas	ELECTRONIC SYSTEMS TECHNOLOGY OFFICE (ESTO) Research Areas	SOFTWARE AND INTELLIGENT SYSTEMS TECHNOLOGY OFFICE (SISTO) Research Areas
Warbreaker Command and Control Warfare Advanced Distributed Simulation Special Projects Military Operations in Built-up Areas Warfighting Systems	Defense Technology Integration and Infrastructure Defensive Information Warfare National-Scale Information Enterprise Networking Systems Scaleable Systems and Software Microsystems	Display Technologies Tactical Information Assistants Microelectro-mechanical Systems Microwave Technologies Rapid Prototyping of Application-Specific Signal Processors	Joint Task Force Advanced Technology Demonstration Demo II: HMMWV Surrogate Vehicle

DEFENSE SCIENCES OFFICE (DSO) Research Areas	MARITIME SYSTEMS TECHNOLOGY OFFICE (MTO) Research Areas	SENSOR TECHNOLOGY OFFICE (STO) Research Areas
Materials Applied Science	(No information available)	(No information available)

Source: ARPA Home Page (prior to August 8, 1995)

On August 8, 1995, ARPA reorganized its technical offices to form a new Information Technology Office (ITO). The ITO is now responsible for research into "breakthrough information technologies for potential use in advanced defense applications." The ITO consists of program managers and programs drawn from the former CSTO, SISTO, DSO, and MTO offices.

2. Example Technology Research Areas

a. Artificial Neural Network Technology

Artificial Neural Network Technology (ANNT) will potentially revolutionize information processing for pattern classification and autonomous control. The ANNT program is demonstrating the utility of neural nets (as contrasted to conventional approaches) for a variety of military applications, developing hardware implementation technologies, and exploring advanced ANN architectures for future system improvements.

b. Broadband Information Technology (BIT)

This program is to develop and demonstrate key enabling technologies for terabit optical fiber networks with global reach meeting critical DoD needs in the year 2000 and beyond. Optical fiber is the transmission medium of choice for broadband networks, owing to the 30 THz bandwidth of its low-loss transmission windows. At present, fiber networks only use at most 1 percent of this potential capacity because of electronic bandwidth limitations, not of the fiber, but within the network itself and at the user access points. The BIT program aims to develop the advanced network technologies, architectures, and protocols to access the 30 THz bandwidth utilizing multiple channels (wavelengths) and pico second optical pulses.

c. Defense Information Enterprise Technologies

The Defense Information Enterprise Technologies (DIET) program develops the underlying computing systems' technology that enables applications developers to demonstrate prototype solutions to national- and global-scale defense programs. These solutions will provide the technological basis for an infrastructure based on commercially available technology enabling defense needs to be satisfied.

d. Defense Technology Integration and Infrastructure

The ITO Defense Technology Integration and Infrastructure program (DTII) is intended to help transition advanced technologies sponsored by ARPA offices into the defense mainstream by developing the unifying glue or integration technology that can bring technologies developed by ARPA and other agencies together into common systems frameworks.

e. Education and Training

Readiness is one of the critical issues facing DoD. The advancements in and complexities of modern weapon systems, C4I, medicine, vehicles, and support systems require increasingly sophisticated (and costly) training for individuals. The Computer

Assisted Education & Training Initiative (CAETI) will provide enhanced learning capabilities for DoD.

f. Information Survivability

The Information Survivability program creates advanced technologies to protect DoD's mission-critical capabilities against electronic attack upon or through their supporting computing infrastructure. The goal is to create affordable, verifiable, scaleable technologies for a robust and secure defense infrastructure through configurable replaceable components and robust system design technology.

g. Intelligent Systems

The ARPA investment strategy for Intelligent Systems focuses on advanced representation and reasoning techniques to make military software systems easier to use and more capable of supporting operators in completing their missions. The 10-year challenge is to make systems smart enough to perform as capable and taskable associates for military personnel and operational groups. The nearer term goal is to develop advanced software systems that perceive, plan, and act to provide improved capability for military users and autonomous systems in areas of crisis management, intelligence processing, and manufacturing. ITO's Intelligent Systems programs are Human Computer Interaction and Human Language Systems.

h. Microsystems

Microsystems is responsible for critical aspects of the science and technology that enable the design, development, manufacture, and application of advanced microsystems for basic research through small-scale prototyping. A key focus is high performance, densely packaged, low power, scaleable components relevant to defense needs that can be accurately simulated, realized in advanced implementation technologies, and rapidly designed into candidate architectures, considering both hardware and software.

i. Networking Systems

The Networking Systems program develops critical technologies necessary for the Department of Defense to carry out its mission. Of utmost importance is the capability to communicate on a global scale, across an extremely diverse set of communication systems, and with the highest reliability and performance in an affordable manner.

j. Scaleable Systems and Software

The Scaleable Systems and Software program supports the development of computing and advanced software technologies needed to enable the development, introduction, and effective use of secure scaleable and distributed high performance computing technologies. The technologies developed by this program drive U.S. military capabilities in areas such as target recognition, synthetic theaters of war, submarine propeller design, and many others that benefit from the ability to do complex modeling and secure distributed communication.

k. Software Engineering

The goal of programs in software engineering is to reduce the cost and risk of creating new military systems and to enable their affordable modification to meet new and unanticipated missions. Even if DoD were never again to procure new custom software, this need would persist; both the current body of existing legacy systems and any new COTS systems need to evolve as needs and missions change. In addition, DoD software, is unique in functionality (it is unlikely that there will be a COTS mission guidance system), real-time requirements, and life-criticality and in the longevity of the systems' deployment. These programs are designed to develop and transition technology that will meet these unique needs.

l. Systems Environments

The ARPA Systems Environments program supports the development of the advanced software technologies needed to both enable and accelerate the development, introduction, and effective use of scaleable high-performance computing technologies. This program supports the Advances Software and Algorithms component of the Federal HPCC program.

E. DEFENSE AIRBORNE RECONNAISSANCE OFFICE (DARO)

1. Overview[3]

The DARO serves as the DoD's Office of Prime Responsibility (OPR) for airborne reconnaissance as well as the development and execution of action plans to meet reconnaissance requirements in collaboration with OPRs for weapons, imagery intelligence (IMINT), signals intelligence (SIGINT), measurements and signatures intelligence (MASINT), and human intelligence (HUMINT). The DARO itself is a development and acquisition organization staffed jointly by the Under Secretary of Defense (Acquisition and Technology) [(USD(A&T)] and the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) [ASD(C3I)]; the DARO's Director reports to the Deputy Under Secretary of Defense (Advanced Technology) [DUSD(AT)]. Executive-level oversight and guidance are provided by the Defense Airborne Reconnaissance Steering Committee (DARSC), now chaired by the USD(A&T) whose membership is DoD-wide. Figure 3 sets forth these organizational relationships and DARO's internal structure.

---

3 The DARO material is extracted from DARO's document *Airborne Reconnaissance Technology Program Plan, Executive Summary*, distributed in the summer of 1995.

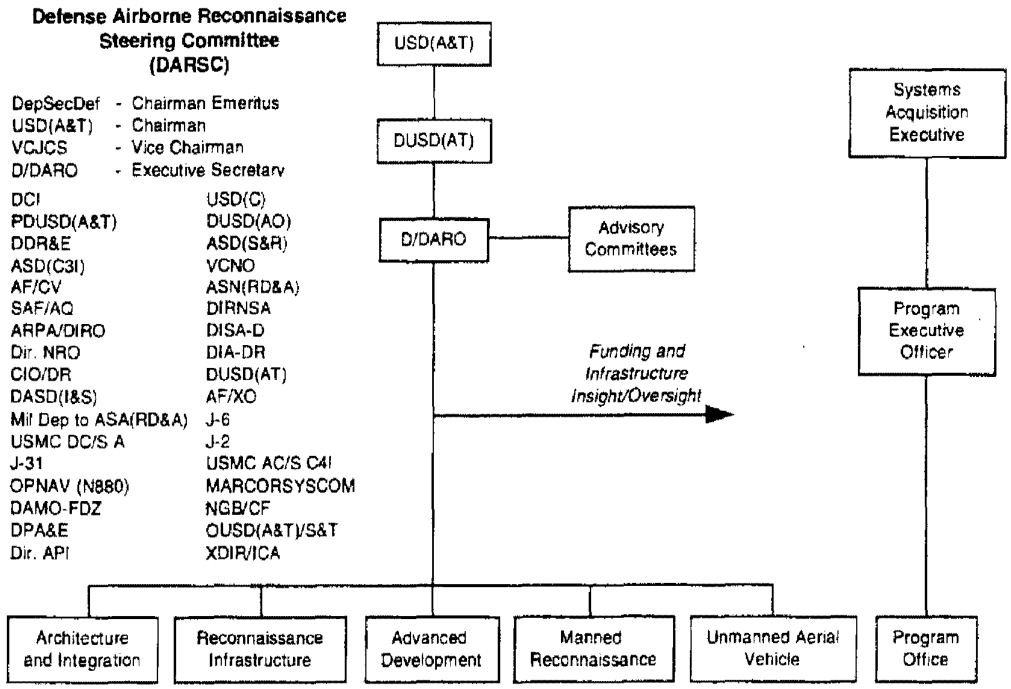


Figure 3. DARO Organization

The DARO has recognized that, in order to migrate to a Defense-wide objective architecture, the entire airborne reconnaissance community needed a systematic and comprehensive approach to selecting, developing, and deploying specific airframe, sensor, information processing, and communications technologies to support an Objective Architecture. The approach to technology development would need to be built within the context of diminishing DoD resources and be able to tap into the broad base of both Government and commercial technology investments. Accordingly, the DARO conducted a study that involved representatives from the Services, the defense agencies, national laboratories, industry, and academia to identify the requisite technologies and focus their development into a planning structure designed to support long-term airborne reconnaissance capabilities. Areas highlighted for improvement in the current reconnaissance capability that were documented in the DARO Integrated Strategy, and recently emphasized by the *Intelligence Bottom-Up Review* were the following:

- Continuous broad area coverage
- Higher-resolution data to support precision strikes
- Improved sensors for battle damage assessment
- Improved over-the-horizon communication and connectivity
- Increased communication bandwidth
- Better information retrieval and distribution

- Comprehensive source correlation
- Synchronization with warfighter needs.

Those improvements are part of one of the five Future Joint Warfighting capabilities most needed by the U.S. Combatant Commands, specifically (in the words of the Joint Requirements Oversight Council [JROC])": ...To maintain near perfect real-time knowledge of the enemy and communicate that to all forces in near-real time."

The DARO Technology Plan, therefore, presented an investment strategy that was developed to support the goal of extended reconnaissance--the ability to supply responsive and sustained intelligence data from anywhere within enemy territory, day or night, regardless of weather, as the needs of the warfighter dictate. It is a stepping stone from DARO's *Integrated Strategy*, which introduced this goal, to actual implementation of a unified approach to development of capabilities for our future joint reconnaissance force mix. The key to this transition is investment in technology areas that will enable us to get the most from research and acquisition efforts at the lowest cost. These are listed below.

2. DARO's Technology Thrust Areas

a. Low-Cost Reconnaissance Pod

Pod-mounted sensors offer a flexible approach to airborne reconnaissance by reducing reconfiguration time and by allowing a single hardware configuration to support multiple missions. The DARO feasibility study will bound program costs and schedules, will establish reasonable weight and size constraints, and will ensure that resulting pod systems are common and interoperable. This study will be coordinated with the Services, in light of the Air Force Air Combat Command's Theater Airborne Reconnaissance System (TARS) and the Navy/Marine Corps' Advanced Tactical Airborne Reconnaissance System (ATARS).

b. Integrated Avionics

Avionics technology is going through revolutionary changes. DoD-integrated avionics programs are developing technology that promises to increase the performance of manned aircraft dramatically, while reducing cost and weight. To accomplish this, avionics subsystems, including vehicle and mission subsystems, are linked through a digital data network to an integrated processor. In addition to cost savings from the use of shared components, Avionics integration is expected to improve reliability, increase payload capacity, and allow flexible operations with Allied systems on a worldwide basis. With a goal to develop improved avionics systems for unmanned aerial vehicles (UAVs), the DARO Integrated Avionics program will build upon progress made by the Joint UAV Project Office's Modular Integrated Avionics Group (MIAG) program, and by ongoing DoD and National Aeronautics and Space Administration (NASA) manned aircraft avionics efforts. A program plan will be developed to direct work on issues such as integration of vehicle avionics, mission avionics, primary flight control avionics, and threat warning with the goal of progressing toward a totally integrated, open architecture system for future UAVs. Hardware/software breadboard efforts will address issues associated with application of the considerable advancements in manned aircraft avionics to UAVs.

c. Exigent Target Detection

The Exigent Target Detection program seeks to develop sensor technology that improves detection of buried, hidden, or camouflaged objects. The first effort in a series of thrusts will build upon multi-spectral imaging (MSI) upgrades to the H-camera sensor improvement program (H/SIP) and to the Senior Year Electro-optical Reconnaissance System (SYERS), both slated to start in FY 1995. The end product of the MSI thrust effort will be a demonstration of multi-spectral detection and identification capabilities in a military exercise. Programming of follow-on thrusts will be determined by technology state of the art and by closer examination of relevant IMINT and MASINT technologies, such as infrared (IR) MSI, multi-phenomenology systems, foliage penetration synthetic aperture radar (FOPEN SAR), and laser radar.

d. Precision Geolocation

The Precision Geolocation program develops sensor technology enabling airborne sensors to measure the earth-centered geo-coordinates of targets and features on the ground. Designed as a series of thrusts, this area begins with demonstration of electro-optical (EO) and/or SIGINT geolocation with an accuracy goal consistent with Global Positioning System (GPS)-guided precision guided munitions (PGMs). The use of Differential GPS or carrier-phase tracking GPS capabilities will also be considered in the first phase of the program. Follow-on activities will examine the technology options for SAR geolocation or more precise EO/SIGINT geolocation possibly employing fiducial-reference unattended group sensors.

e. SIGINT Technology

The SIGINT Technology program will develop advanced technologies to address several emerging challenges in the SIGINT area. Technologies of potential value to this program include sensor networks of opportunity (cross-program SIGINT), signal-specific technology developments, and electromagnetic compatibility and interference canceling among system components on a multi-function platform. New and experimental technologies relevant to airborne SIGINT will be fielded as prototype capabilities on a limited set of platforms to determine their utility before integration into airborne reconnaissance fleets.

f. Imagery Screening and Analyst Cueing

The Imagery Screening and Analyst Cueing effort will include the evaluation, simulation, and demonstration of algorithms for imagery screening and analyst cueing. Algorithms with high potential for useful application will be demonstrated using special enhancements to existing Advanced Distributed Simulation (ADS) capabilities. The simulations can be supported by a library of stored image chips, although the more expensive and involved approach of real-time, high-fidelity image simulation provides greater flexibility. The algorithms that demonstrate suitable utility to the warfighter in the ADS demonstration will be applied to both onboard and on-ground demonstrations. These demonstrations will incorporate expected advances in high-speed compact processors, solid-state data records, and common ground stations. A successfully demonstrated imagery screening capability will provide additional data handling alternatives to airborne platforms and will improve the effectiveness of imagery analysts.

g. Automatic Target Recognition (ATR) and Correlation

The ATR and Correlation Technology effort will evaluate algorithms for utility to the warfighter, coordinate further algorithm development by the DoD community, simulate the algorithms, and demonstrate them. The simulation will be accomplished by special hardware and software enhancements to the existing ADS capability. The algorithms that indicate a high degree of utility in the simulation will be demonstrated in a "live" onboard scenario, leading to algorithms well suited to the warfighter's needs. Onboard demonstrations of ATR and correlation algorithms will benefit from the expected advances in high-speed compact processors, parallel algorithm designs, and solid-state data recorders. This program will result in ATR and correlation algorithms ready for application in reconnaissance systems to improve the information value of the data provided to the warfighter.

h. Common Data Link (CDL) Advanced Technology

The CDL Technology program will pursue several advanced technologies that can provide long-term cost savings in the CDL program, to include the development of a Government covert waveform, insertion of COTS technologies, improved manufacturing technology, and information technologies for increased flexibility in the use of the CDL.

i. High-Data-Rate Uplinks and Crosslinks

The High-Data-Rate Uplink and Crosslink programs are designed for orders-of-magnitude enhancements needed for next-generation sensor data rates. The technology program will focus on gigabit crosslink and uplink rates from high-altitude platforms such as the U-2 and High Altitude Endurance (HAE) UAV. EHF and laser communications provide jam-resistance and opportunities for smaller size, weight, and power necessary for endurance UAVs. EHF uplinks will depend on the future availability of UHF payloads on satellites. Technology development will involve partnership with NASA, the Services, and the commercial sector analogous to the near-term Commercial Satellite Communications Initiative (CSCI). The crosslink program will foster a frequency competition between EHF and lasers to produce the most affordable lightweight system. The results of statistical meteorological studies and advances in conformal antenna technology will be incorporated into the program. Laser communication is a high-risk, high-payoff area whose risk will be mitigated by a series of technical demonstrations.

APPENDIX A
RAPIDITY OF CHANGE OF INFORMATION TECHNOLOGY

Appendix A

RAPIDITY OF CHANGE OF INFORMATION TECHNOLOGY

Today information technology is changing at an enormously fast pace. Like any other massive human enterprise, information technology, which is coming of age at this point in time, results from an amalgamation of many different threads affecting our culture with origins that can be traced back to the dawn of history. Two of the major threads that lead to information technology are communications and computing.

As we enter the 21st century, civilization is entering a new technological state that is dramatically changing the way we do business. The rush towards this information revolution, akin to the Industrial Revolution, is centered in the United States and has been steadily growing since the middle 1950s. Future historians will very likely consider the first decade of the 21st century as the beginning of the information revolution.

A. MODERN ORIGINS

Returning to the two primary components of the information revolution, the earliest modern origins of communications can be traced to the second half of the 19th century. James Clerk Maxwell's understanding of electromagnetism (1867), Alexander Graham Bell's invention of the telephone (1876), and Guglielmo Marconi's invention of the radio (1896) were all major predecessors of the wired and electromagnetic transmissions of signals that make modern communications possible.

With respect to computing, although one might find earlier origins in the computing engines of the 19th century, e.g., Charles Babbage (1833), the truly modern origins are 20th century events. These start with the differential engine (1931) of Vannever Bush and the digital concepts and implementations (early 1940s) by Alan Turing, Eckert & Mauchly, and John von Neumann.

The modern implementation of these two threads rest on common technology, initially the vacuum tube, invented by Lee DeForrest (1906), then the transistor by Bardeen, Brattain, and Shockley (1947), and finally the integrated circuit invented independently by Robert Noyce and Jack Kilby (1956). The real growth has come in the evolution of the technology of the integrated circuit through its many variances and increasingly larger scales of integration.

B. CURRENT TECHNOLOGY

The rapidity of change that has occurred and continues today is demonstrated with a study of the recent history of the communications technology thread (today's Internet) and also the trail of commercial computer equipment milestones, beginning with the latter half of the 1950s, which is when the modern rapid rate of change started. Table A-1 traces that history starting with the early idea of interconnecting the country's computers together to form a computer utility that was generated in 1957 at MIT. It then traces some of the important technical, funding, and legislative events, which gave rise to the Internet as the current instantiation of the National Information Infrastructure (NII). Similarly Table A-2 shows some performance parameters for a sampling of the computers that have been important milestones in the growth in the commercial computer industry starting with the IBM 704, first delivered in 1957, through today's Pentium chip based personal computers (PC).

Table A-1. Internet History

Date	Event
1957	Corbato & McCarthy: Computer Utility (MIT)
1960s	Packet-switching networks (RAND)
1969	ARPANET commissioned by DoD
1970s	Store and forward networks
1982	Transmission Control Protocol (TCP)/Internet Protocol (IP)
1983/4	INTERNET created; Domain Name Server (DNS) introduced
1986	NSFNET created; part of HPCC program
1987	Merit Network, Inc., contracted to manage NSFNET
1990	ARPANET ceases to exist
1991	"Gore I" establishes NREN; World Wide Web introduced
1992	NSFNET upgrades from T1 to T3
1993	"Gore II" establishes NII; NSFNET operation contracted out
1994	Mosaic (U of IL) 1.5M accesses/week

Table A-2. Commercial Computer History

Year	Processor	Technology (CPU/Mem)	Cycle (ns)	Memory Size (MBytes)
1957	IBM 704	Vacuum tubes/core	12,000	0.19
1962	PDP-1	Transistors/core	5,000	0.03
1964	CDC 6600	Transistors/core	1,000	1
1965	IBM 360/75	LSI/core	400	1
1974	Cray 1	ECL/Bipolar (1 Kb)	12.5	8
1976	Apple 1	4-bit PE/DRAM (1Kb)	1,000	0.05
1986	Cray 2	ECL (16 Gate)/DRAM(1Mb)	4.1	200
1992	Cray C90	ECL (10K Gate)/Bi CMOS	4	2,000
1994	"Pentium"	Bi CMOS/DRAM (64 Mb)	10	64

From Table A-2, it can be seen that the 1994 Pentium-chip-based PC, costing less than $5,000, has computing power approximately 1,200 times that of the IBM 704 costing approximately $5 million (1957 dollars). It also comes with a memory capacity up to 300 times larger. Or, if one compares the leading-edge standard supercomputer, i.e., today's 16 processor Cray Research C90, the estimated computing power improvement over the IBM 704 (the leading edge computer of its day) is almost 400,000. The memory ratio is approximately 10,000. However, the most spectacular statistic is the performance per unit cost ratio of ~1,200,000 between today's Pentium based PC and the IBM 704. If this had occurred at a constant rate over the intervening 37 years (which it did not), the performance per unit cost (in dollars of the time) improved better than a factor of 2 every 2 years.

Since early in the 1960s, almost all growth and rate of improvement have been based on silicon semiconductor technology. Improvements have occurred with a natural growth in understanding of the science, technology, and art involved in the complex processes involved. Some of the most recent progress has been made with the introduction of gallium arsenide as the semiconducting element, but this is unlikely to affect the primary reliance on silicon-based devices for commodity parts.

In the mid-1960s, Gordon Moore, one of the pioneers in this industry, noticed that the number of components per chip in the most advanced integrated circuits were doubling every year and that the expectation was for the trend to continue into the future. This observation (sometimes called Moore's law) turned out to be not quite correct. As with all technologies, rapid growth cannot be sustained indefinitely and a slowdown has occurred, starting in the early 1970s. Today the doubling time is closer to 2 years--still a spectacular rate of improvement. However, one must expect saturation effects to continue to slow the rate of change until a totally new technology emerges. Figure A-1 gives a summary of this improving technology accomplishment, characterized by the chip feature line widths (the thin line-right axis) and with milestones (the thick line-left axis) in commodity DRAM and processor chip products. Notice that the line width on the chips has been steadily decreasing but, as the limits of the wavelength of light are approached, the technology is approaching the diffraction limits of visible light, and consequently the rate of improvement is decreasing. Other techniques must be developed for producing the masks to continue to decrease the feature line width.

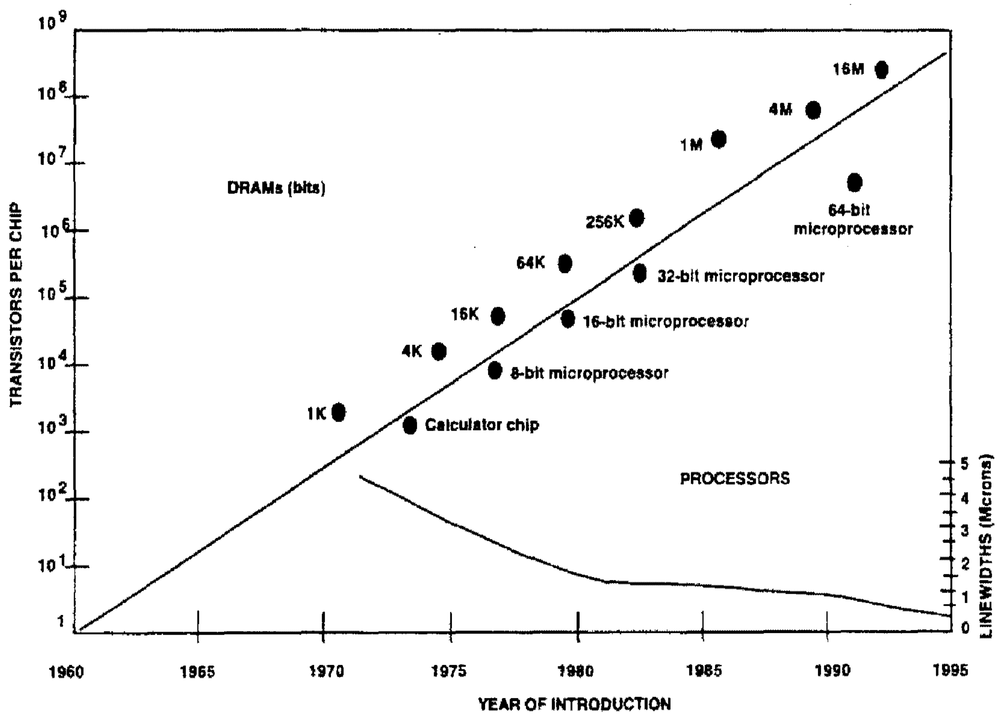


Figure A-1. Evolution in the Scale of Integrated Circuits

Just as processor and memory improvements have been based primarily on silicon technology, magnetic systems have been the technology of choice in secondary storage media. Although for some functions optical disks and, more recently, optical tape appears more appropriate, most storage systems in operation today use magnetic media as the storage element. Magnetic disks became the standard online mass-storage element in the 1960s. At that time, typical area storage densities were 100,000 bits/in^2 and the storage capacity was about 5 MB/spindle. Today much improved versions of the technology have storage densities approaching 1 Gb/in^2 and storage densities approaching 5 Gb/spindle.

For off-line storage, magnetic tapes continue to be the standard as they have been since the mid-1950s. At that time typical lineal densities were 200 bits/inch and densities were 2,800 bits/in^2. This had increased to 6,250 bits/inch and 112,500 bits/in^2 when GCR encoded tapes were introduced in 1973. And, today linear tapes are capable of 20,000 bits/inch and 1 Mb/in^2.

Projections for the future are for continued increasing densities and further miniaturization. Thus, one will continue to see magnetic technology used for online disks. For the "near-line," off-line, and archival storage systems, the choices today are primarily linear tapes, with robotics for the larger systems. Digital helical scan tape (i.e., video) technology is rapidly developing and will very likely become the technology of choice for near-line and off-line storage in the near future. The linear densities attained with this technology exceed 50,000 bits/inch and the densities approach 100 Mb/in^2. Also, especially for widely distributed and relatively static databases, the CD-ROM is ideal technology and its use will continue to increase at a very high rate.

C. COMPUTER SYSTEMS

With respect to the growth of computer system equipment technology, Figure A-2 is a summary graph of this technology during the modern period. Here the upper line represents products leading the technology, typically the "supercomputer" of the day, and the lower curve represents an affordable state-of-the-art system that is a functional system capable of providing useful work in almost any reasonable context. Milestone commercial products are listed on these curves and in the upper and lower portions of the curve are milestone bullets indicating the occurrence of important computer-related events, either software, communications, or legislative. Some DoD milestones are also listed.

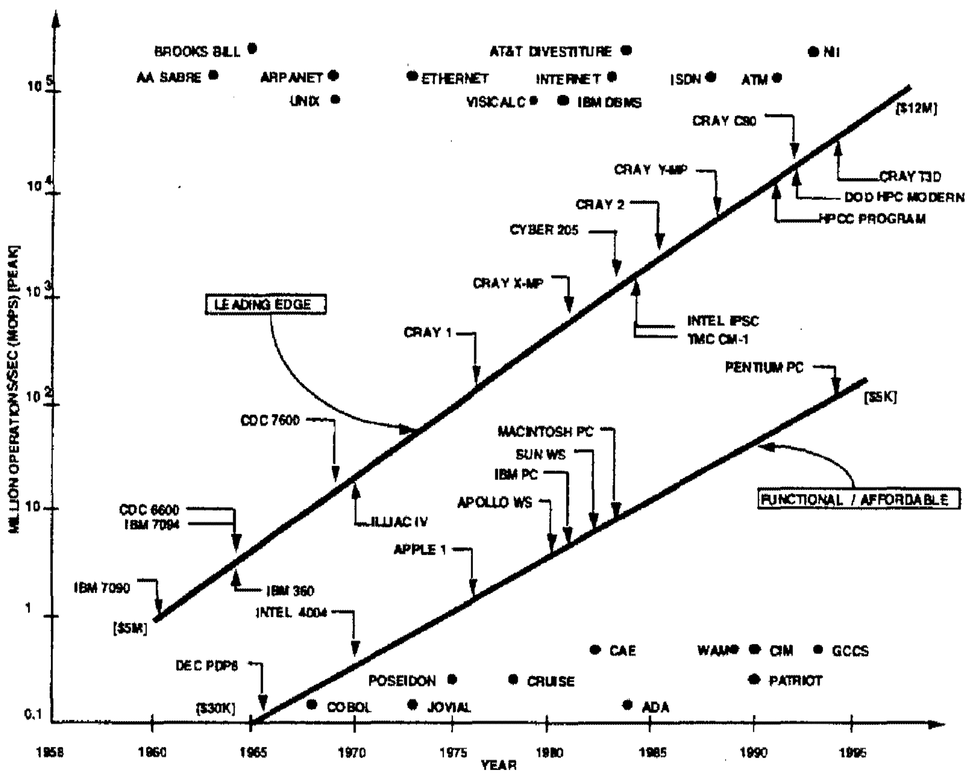


Figure A-2. Growth of Computer Technology

An important aspect of computing technology is software. Enormous gains have been made since the mid-1950s, but the measures are much more difficult to assess, and the culture is much closer to an art than an engineering discipline. With every improvement in hardware performance, concurrent improvements in software have also occurred. Improved algorithms and programs perform functions more efficiently and/or more extensively, compounding the performance improvement of the hardware. Operating systems continue to become more powerful and effective, performing an extending class of service functions for the user. Compilers become more efficient and capable of mapping source language programs onto a growing range of different computer architectures. Productivity enhancing tools, e.g., software engineering tools, are becoming increasingly effective. As a broader user community with an increasingly wider range of application needs has appeared, commercial enterprises satisfying these needs have blossomed. Here is where the commercial off-the-shelf (COTS) approach to technology insertion reaps great benefits. Probably the most important progress in software technology has been the transformation that these advances have brought about in the way computers are used. Rather than the simple replacement of human work effort by a machine emulating the human process, wholly new activities are enabled, e.g., virtual reality experiences.

Enormous unseen needs properly require more computing capability. These include the human-computer interface that is computing intensive and becomes more and more important as the interface becomes more human-natural. Each release of a new generation of personal computers generates new software products, which very quickly exhaust the additional capabilities that the new hardware products bring. Invariably this makes obsolete previous generations of hardware products that no longer have the CPU or memory capabilities to run the new generation of software products.

As more and more information retrieval capability is made available, especially in the command and control context, larger random access storage systems will be required, both directly addressable and in the online or near-line electromechanical storage elements. Distributed information retrieval systems require much higher bandwidths for the storage and access of data. A transition is occurring in the use of Small Computer System Interface (SCSI) and other bus-based technologies to fiber channel that is currently the preferred technology for this function.

D. FUTURE COMPUTING TECHNOLOGY

As new computing systems are designed, many design and technology considerations must be examined. The classic von Neumann single-processor stored program machine is reaching technological limits. Limits imposed by the speed of light, the uncertainty principle, diffraction effects, and limits on the materials being used will soon begin affecting the rate of improvement possible based solely on improvements of the technology. There may yet be factors of 10^2 or 10^3 to be gained this way as the technology is further refined, but factors of 10^6 will not be available without new technology. Many of the changes that are occurring and will enable further advances are in the architecture. In the 1960s, vectorization was introduced. This brought improvements over scalar machines, for those problems appropriate to vectorization, of up two to three orders of magnitude. This technology is now mature and works quite well. However, it too is reaching its limits. Consequently, one must turn to parallelism where the problems turn out to be much more difficult than originally perceived when work began in this area in the early 1980s. But, progress is being made on commercial parallel systems, which do work quite well for certain classes of problems. Many of the solutions to the problem of making this work are to be found in the software arena and in understanding appropriate approaches to working in a parallel rather than a serial world.

Silicon is the basic technology of choice for components today, with some use of gallium arsenide and various hybrid processes. These will saturate and to make major gains will require new technology. New approaches that have been tried but not yet successfully used to build major systems include superconductivity and neural nets. At the experimental level, optical technology is also under study. There is no indication within the foreseeable future, that any of these technologies will mature to replace the general purpose component role that silicon plays today. Each does have some role in very special cases. Recently, Leonard Adleman of University of South Carolina (USC) published the results of an experiment using a biological approach to computing. Biological and quantum devices appear to be the most attractive of the totally new technologies for replacing silicon. In his experiment, Adleman constructed a DNA sequence to solve a small traveling salesman's problem. This is a very spectacular demonstration, but biological computing is years away from being a general-purpose widely used technology.

Thus, in the computing domain for the foreseeable future (i.e., the next 20 years), higher performance will be obtained by continuing incremental improvements in silicon and gallium arsenide technology using more and broader approaches to parallel processing.

E. INFORMATION INFRASTRUCTURE

The NII is a web of interconnected interoperable public and commercial private networks. The Internet, which is today's instantiation of the NII, encompasses many thousands of local area network (LAN) nodes, the utility telecommunications networks interconnecting them, the user computers, and, most importantly, the information for which the infrastructure exists. The goal of the NII is to be a ubiquitous and seamless system to interconnect any user to any set of information to which she/he has rights. The start up of the NII can be compared to beginning of the telephone system at the beginning of the 20th century. There the goal was universal service. It has been attained by regulated monopoly, which is now in the process of being dismantled. In contrast, the NII, starting with the ARPANET in 1969 and now transferred into a complex web of up to 20,000 individual networks, is being nurtured by Government in what might be considered a guided, competitive arrangement.

Although initially the primary information accessed and transferred on the internet was textual, as the systems have matured, the bandwidth capability has grown, and a broader spectrum of users are participating; the information exchanged now includes various classes of information with which communications systems have classically dealt. These include voice, fax, both static and dynamic, video, and the integration of these elements in the multimedia environment. Various compression schemes are used to make effective use of the bandwidth, especially with respect to the high bandwidth video signals. One set of problems yet to be solved is the inclusion of appropriate encryption techniques to satisfy both national security issues at all levels as well as proprietary and privacy matters.

F. NETWORKING TECHNOLOGIES

The networking links, which compose the Internet, use a very large group of switching and transmission technologies. Some of these emanate from the telecommunications industry and some derive from the computing community. For example, with respect to data transmission protocols from the communications community, there are X.25, ISDN, BISDN, frame relay, ATM and SONET protocols. From the computer community, there are SNA, TCP/IP, Ethernet, FDDI, fiber channel and HiPPI protocols. The appropriate mixing of these protocols in a seamless unified system requires additional maturation of the technologies.

For the interconnection of dispersed nodes, i.e., the wide area network (WAN) elements, analog modems using switched telephone lines operating at 2,400 baud was state-of-the-art in the 1960s. Improvements in modem technology increased the performance of these systems from 2,400 to 9,600 Kbaud on switched lines and to 56 Kbaud on dedicated lines in the 1970s. In the early 1980s T1 (1.544 Mbps) became available for dedicated connections. T3 (45 Mbps) is now the current public-utility state of the art. With the advent of optical fiber, OC3 (155 Mbps) is becoming generally available, and, in some locations, OC12 (620 Mbps) and even OC48 (2.48 Gbps) connectivity is available. This enormous increase in the available bandwidth has been an important part of the driving forces that have made the concept of the NII possible.

It is in the transmission lines that optical technology has made a spectacular improvement over the previously available twisted pair and coaxial line technology. Fiber optics is inexpensive, has low transmission losses, and has very wide bandwidth capability. Furthermore, it is much more robust from a security point of view.

Transmission services available today include those supplied by the local and long distance telephone, cellular phone, and cable companies. However, there is a rapidly growing industry to supply satellite-based communications services. In addition to the number of geostationary earth orbit (GEO) satellites, a large number of low earth orbit (LEO) satellite systems are now being planned and, in some cases, are already installed. The advantages of the LEO system is that the transmission delays are low due to the proximity of the satellite orbit to the earth and that the power required for successful signal transmission is much lower. Many of the systems being planned are aimed at the personal mobile digital telephone market, requiring between 10 Kbps and 64 Kbps per channel. Such systems operating in the low GHz frequency range, e.g., the Motorola Iridium or the LQSS Global star systems, will make possible mobile interconnections any place on the surface of the earth at these bandwidths. These systems are very large and are multi-billion dollar investments requiring several dozen satellites in orbit to accomplish the mission. The most aggressive of the systems in the planning stages is the Teledesic system with a proposed 924 satellites working at a very high bandwidth (~20-30 GHz). The investment for this system, which is aimed at the data market with high bandwidth for each individual channel, is projected to exceed $9 billion.

The major technological problem ahead is to develop approaches to weaving these various services into a seamless whole so the data can be moved from any point A to any point B using whatever assets are most appropriate for the connectivity in a way that is transparent to the user. Many of today's ongoing activities are slowly solving those problems. It will probably be well into the first decade of the 21st century before many of these goals are achieved.

G. THE FUTURE

Electronic technology giving rise to 10^9 component chips, thereby allowing for gigaflop processors and gigabit memories, will make the information revolution possible during the first decade of the 21st century. Likewise, communications technology (which by that time will be almost all digital) will use an extensive fiber optic infrastructure coupled to the extant copper and coaxial cable infrastructure LEO satellites with an interoperation of all these communication assets. The most dramatic transformation will not be technological but an organizational one. The intermingling of the telephone, cable, and cellular companies with each other and with the broadcast industry and others not as easy to identify will make up for the corporate enterprise that will be in a position to make all of this available. Government policy and actions in a number of different domains including intellectual property rights, regulation, privacy, and security must be addressed. But, if all is in place, the information revolution will affect in a most dramatic manner the way in which society will do its work.

(This page is intentionally blank.)

APPENDIX B
DISTRIBUTED COMPUTER NETWORKS

Appendix B
DISTRIBUTED COMPUTER NETWORKS

A. INTRODUCTION

The last decade has seen the advent of a new era in applications of information processing and transmission capabilities. The emergence of the Internet computer-to-computer network[1] stemmed from the following:

- Incorporation of multifunctional capabilities in low-cost computers
- Availability of affordable equipment for transmission of digital data over public telephone networks
- Development of systems and standards, under the ARPANET program, that supported the concept of a universally accessible information exchange system.

As was mentioned in Appendix A, Internet is now a complex, worldwide network of networks, with important implications for the academic and commercial worlds, as well as the public at large. The original concept of information access and exchange has expanded to include new distributed computing functions, including transactions, multi-media processing, and distributed artificial intelligence (DAI). The advent of the new functionality created by distributed computing concepts has given rise to new technical issues, but important concerns also exist with regard to protecting information and user interests. This appendix provides three summary analyses of some major issues and implications in the area of distributed computing and concludes with a brief description and analysis of the DoD Goal Security Architecture (DGSA). Security, as used in this appendix, pertains to providing data confidentiality and integrity as well as system integrity and availability.

[1] Although computer-to-computer networks were in use before the advent of the Internet, they were generally systems dedicated to specific organizations or functions.

A. DISTRIBUTED OPERATING SYSTEMS

1. Background

Operating systems provide the interface between functionalities embodied in application software and the hardware functions of the computer. They govern the capability of the computer to use computational hardware, storage capabilities, and input/output resources efficiently, and the range of functions, from user-oriented applications to system control and file management, that can be supported. They are a basic determinant of system performance, can profoundly influence computer-to-computer and human-to-computer interactions, and play a fundamental role in information security assurance. The core (kernel/micro-kernel) of an operating system can provide the essential separation mechanism need to enforce security policies at the read/write/execute instruction level.

Distributed operating systems form the core of the computing and communications system infrastructure. The challenge to achieve maximum performance, assure effective element-to-element interactions, and support acceptable levels of information security is greatly magnified by the diverse and heterogeneous nature of the infrastructure and its components.

2. Technology Trends and Status

The following three major trends will shape distributed operating system technology in the future:

- The demand for greater real-time, reliable performance, to support distributed multimedia applications--With the advent of very wide addressing schemes, e.g., 64-bit addressing, the ability to exploit virtual addressing concepts and provide persistent objects in distributed systems is improved.
- The emergence of object-oriented technologies--New paradigms of service, such as object brokering, are being developed. The advent of agent-oriented software and DAI programs will further expand the dynamic adaptation capabilities of distributed operating systems.
- The advent of nomadic computing--The examination and closer coupling of networking protocols with operating system micro-kernels will yield new views of networked operating systems.

All of these technologies are converging in the field of operating systems research and will result in better understood, better constructed, and better performing operating systems in the future. The future operating systems will have sufficient intelligence to be able to adapt to a variety of operating environments.

Commercial demand for improved operating system capabilities is high, and vendors, universities, and Government agencies continue to spend large sums to gain the improvements that are demanded. The operating systems of today are just beginning to achieve the capabilities of fully distributed operating systems. Most fielded configurations are stand-alone systems with networking capabilities to conduct file transfers. Most distributed operating systems currently being fielded have the capability to interact with existing systems using existing file exchange procedures, but cryptography issues may cause interoperability problems.

Development of distributed operating systems is being accomplished by a diverse and robust research community with significant challenges to meet. Software tools and techniques to analyze and develop operating system capabilities have been greatly improved, and improved operating system products are being fielded COTS systems with fair regularity.

Future distributed operating systems will be more object-oriented and network-like, with task-oriented, adaptable agents to extend their capabilities for:

- Nomadic computing
- Electronic commerce
- Rapid and interoperable configuration of heterogeneous system components
- Information discovery.

These operating systems will be object-based, task-oriented, protocol-driven, and directory-supported. Protection will be provided by strong encapsulation, with domain and type enforcement, and "negotiated" security protocols. Hardware mechanisms and cryptography will be central to the achievement of such security.

The following are key issues for distributed operating systems research:

- Increased complexity, resulting from efforts to try to do more in the operating system itself. The complexity issue can be mitigated to some extent by modularity, but generally at a cost to performance.
- Scalability, in particular the need for operating system components that enable the management over large and heterogeneous distributed systems
- Information protection functionality, the cost of performance resulting from incorporation of protection mechanisms, and the cost to the vendor for providing necessary assurances that the protection functionality provided is correct.

The major technological risk confronting the fielding of distributed operating systems is the incorporation of cryptographic functionality. The issue of "trust" associated with cryptographic certification authorities is crucially important and must be resolved in a manner that allows international interoperability while preserving the security and policies of participating nations.

B. DISTRIBUTED MULTIMEDIA PROCESSING

1. Background

Distributed multimedia applications will drive computing and communications technology over the next decade. They will require increased access to reliable, high-data-rate service in the networking infrastructure, and reliable real-time processing in workstations. Fundamental changes will be needed in operating systems, to accommodate low-latency, continuous media (e.g., audio and video streams) processing, and asynchronous video-on-demand requirements.

The processing model to meet these requirements will be based on adaptive resource management with deterministic execution. The use of ATM technology, rate-based execution (RBE) schedulers, quality-of-service guarantees, and high-speed agile encryptors will provide the requisite technology base.

2. Technology Trends and Status

The rapidly converging technologies necessary to support distributed multimedia processing will, over time, significantly change the nature of our computing and communications system infrastructure,[2] especially the structure and association of provided resources and services. The technologies' strengths will be manifested in advancing the modes of human-to-computer interactions, to enable the following:

- Real-time video conferencing
- Collaborative workflow
- Compound documents
- New spatial and temporal analysis tools
- Virtual reality.

---

2 This infrastructure includes the operating systems, networking equipment and software, database management systems, human-to-computer interfaces, and systems management and user applications.

Distributed multimedia processing can be used to support information warfare in many ways. Important IW functions that will be enhanced with the advent of distributed multimedia processing technology include the following:

- Real-time teleconferencing
- Rapid situational analysis and awareness
- Large-scale, collaborative planning, design, and command-and-control efforts
- Psychological operations or perception management.

Many of the technological components needed to implement distributed multimedia processing is commercially available as proprietary products, and efforts are underway in the commercial sector to synthesize these components in various forms. However, the synthesis of supporting technologies to enable distributed multimedia processing remains largely in the research arena. The synthesized technology has not been put through sufficient operational testing, and many rough spots will appear, indicating faults, unpredicted performance characteristics, or simply lack of research in particular areas. "Early adopters" are needed to provide the operational feedback necessary to improve the component technologies as well as the synthesized technology.

Distributed multimedia processing is not fully compatible with the current operating environment. Two major missing elements are adequate bandwidth and the capability to process continuous media in real time with appropriate guarantees of fidelity and reliability.

The issues of security in multimedia processing have not been addressed except in some limited aspects of supporting technologies, e.g., ATM agile encryptors. The lack of appropriate protection could preclude the synthesized technology for distributed multimedia processing from becoming an operationally significant resource.

Research is needed on the protection issues of the media forms themselves and their service points, e.g., entry, transmission, processing, display, output transformation, and storage. The issues of security policy and implementation of policy enforcement with respect to media forms and service points are of particular importance in furthering the protection of distributed multimedia processing.

C. AGENT-ORIENTED SOFTWARE AND DISTRIBUTED ARTIFICIAL INTELLIGENCE (DAI)

1. Background

This rapidly evolving technology provides software components--agents[3]--that act on behalf of another agent, such as a human user, or interact among themselves, to perform specifically tailored or heuristically determined tasks. Such agents may be

- Fixed, declarative, or procedural programs, e.g., scripts
- Adaptable, distributed AI systems, e.g., expert systems.

2. Technology Trends and Status

Agent-oriented software and DAI will, over time, significantly change the nature of the computing and communications infrastructure, i.e.:

- Operating systems
- Networking components
- Database management systems
- Human-to-computer interactions
- Systems management applications
- User applications

especially at the interfaces. These changes will occur because the technology can provide responsiveness to heterogeneity, task tailoring, dynamic adaptability, autonomy, intelligence, and cooperative operation. Task-oriented, adaptable agents can extend the capabilities of machine and human resources and could also support a new paradigm in information security.

Agent-oriented software components exist in a number of systems and applications within current operating environments, e.g., MIME messages, WWW Spiders and Robots, and Macintosh Assistants, and are generally embedded within commercial applications or systems. More agent-oriented components are being developed by a growing community of research organizations and commercial software vendors. Research on the use of agents in distributed operating systems is underway.

---

[3] The term " agent" is a poorly defined term with many different interpretations and modifiers leading to a broader inclusiveness of the types of software that compose this technology.

However, the roles and implications of agent-oriented software for distributed systems and DAI have not been fully explored. Issues of policy and implementation with respect to individual and multiple-agent ethics and behavior (collaboration and cooperation, competition, and negotiation) have not been adequately addressed. A critical policy area, protection, is only now beginning to emerge in the DAI research community; here, issues of identification and authentication, authorization, delegation, negotiation, and encapsulation are paramount. Fielding agent-oriented software, as has been done to date, effectively allows the insertion of "Trojan Horse" computer code into client systems with full client privileges because there are few implemented mechanisms such as encapsulation to control or confine the behavior of the agents. It is, therefore, to be hoped that the agents that are in current or near-term use will remain benign.

D. SECURITY ARCHITECTURES

1. Background

The DGSA was developed as part of the Technical Architecture Framework for Information Management to support long-term efforts to achieve DoD-wide corporate information management goals. The DGSA provides the basis for developing security products and mechanisms to be used by system architects, engineers, and integrators to build information systems that meet mission-oriented security requirements.

The centerpiece of the DGSA security concepts, the *information domain*, provides a mission-based approach to the way information is managed and controlled within information systems. A coordinated effort to develop supporting technologies necessary to implement information domains *within a fully distributed systems environment* is essential for making an effective transition from current legacy systems to the DGSA.

2. Technological Components

The DGSA provides excellent security architectural principles and concepts that promote the development of secure information systems by security and systems engineers. The DGSA accomplishes this through the following ways:

- Promoting information protection from a mission-oriented perspective through employment of information domains
- Providing a natural methodology for organizing and separating critical information essential for enterprise operations.

The successful development of information domains depends on three critical technologies: separation technology, security management technology, and security protocols technology.

a. Separation Technology

Implementation of information domains on end systems requires appropriate technological capabilities in hardware, firmware, and software. These capabilities are needed to enforce strict isolation between multiple information domains operating on a single end system and ultimately across a fully distributed network of end systems.

All security-critical functions within the operating system must be isolated from executing instances of information domains. The most promising way to accomplish this isolation is through the emerging micro-kernel operating systems technology. Assurance that the security-critical functions within the operating system are performing properly and (more importantly) not performing any improper activities, is obtained by:

- Minimizing the security-critical sections of the operating system
- Ensuring that the functions are always invoked
- Guaranteeing that the kernel is tamper-proof.

The DGSA will rely on next-generation separation technologies, including advanced hardware and software systems implementations using distributed micro-kernel-based operating systems and memory management facilities employing 64-bit addressing.

b. Security Management Technology

The creation, use, and maintenance of information domains within a distributed network of end systems require effective automated and administrative tools. Security management technology provides critical capabilities to accomplish the following:

- Integrate new information domain security policies
- Maintain security policy rules and attributes for each information domain
- Provide necessary security associations that establish common protection requirements in supporting executing instances of information domains (when communicating across a network).

c. Security Protocols Technology

Security protocols are fundamental elements required to provide a secure transfer system when passing information from an information domain across a network. A secure transfer system is required before creating security associations and providing security association enforcement. Many standards, both commercial and Government sponsored, are already emerging in this critical area.

3. Risks and Risk Mitigation

Current mainstream commercial operating systems are driven by customer demands and do not provide the necessary features to support the DGSA and its information domain construct completely. Lack of systems supporting strict isolation and providing robust security management capabilities is a severe limitation.

Separation technologies, although fundamentally sound, may be difficult to produce on a commercial scale. Security management technology will likely remain expensive because a significant amount of system overhead will be required to achieve full implementation of the DGSA.

Proof-of-concept activities (development and demonstration) are planned for each of the critical DGSA technologies. The goal is to demonstrate that the information domain is a viable construct and that the DGSA can be realized with cost-effective implementations performing at desired levels of efficiency. The proofs of concept and resulting technologies could be used by industry as a basis for developing DGSA-consistent products.

(This page is intentionally blank.)

APPENDIX C
BIBLIOGRAPHY

Appendix C
BIBLIOGRAPHY

A. FUNCTIONAL CONCEPTS

Adleman, Leonard, "Molecular Computation of Solutions to Combinatorial Problems," *Science*, Vol. 266, November 11, 1994.

1992 Annual Report on Scientific Programs, Santa Fe Institute.

"Computing with DNA Could Find Important Future Real-World Applications," *Technology Forecasts and Surveys*, Vol. 27, No. 1, January 1995.

D'haeseleer, Patrik; Forrest, Stephanie; and Helman, Paul; "An Immunological Approach to Change Detection: Algorithms, Analysis, and Implications," submitted to 1996 IEEE Symposium on Security and Privacy, November 10, 1995.

D'haeseleer, Patrik, "A Change-Detection Method Inspired by the Immune System: Theory, Algorithms, and Techniques," Technical Report No. CS95-6, Department of Computer Science, University of New Mexico, November 1995.

Forrest, Stephanie; Hofmeyer, Steven A.; Somayaji, Anil; and Longstaff, Thomas A., "A Sense of Self for UNIX Process, submitted to 1996 IEEE Symposium on Security and Privacy, November 10, 1995.

Forrest, Stephanie; Perelson, Allen S.; Allen, Lawrence; and Cherukuri, Rajesh; "A Change-Detection Algorithm Inspired by the Immune System," submitted to *IEEE Transactions on Software Engineering*, February 20, 1995.

Gifford, David, "On the Path to Computation with DNA," *Science*, Vol. 266, November 11, 1994.

Rogers, Lois, "Science in Two Minds About Artificial Brain," *London Sunday Times*, January 8, 1995.

B. DEVICE TECHNOLOGIES

Amitai, U.; Reinhorn, S.; and A.A. Friesem, A.A., "Visor-Display Design Based on Planar Holographic Optics," *Applied Optics*, Vol. 34, No. 8, March 10, 1995.

Birge, Robert R., "Protein-Based Computers," *Scientific American*, March 1995.

Blaggio, Ivan; Partanen, Jouni; Al, B.; Knize, R.J.; and Hellwarth, Robert; "Optical Image Processing by an Atomic Vapor," *Nature*, Vol. 371, September 22, 1994.

"Cesium Vapor Devices Studied for CPU of Tomorrow's Optical Computers," *Technology Forecasts and Technology Surveys,* Vol. 26, No. 10, October 1994.

DeSouza, E.A.; Nuss, M.C.; Knox, W.H.; and Miller, D.A.B.; "Wavelength Division Multiplexing with Femtosecond Pulses," *Proceedings of the Ultrafast Electronics and Optoelectronics Topical Meetings,* March 13-15, 1995.

Glanz, James, "Will Holograms Tame the Data Glut?" *Science,* Vol. 265, August 5, 1994.

Heanue, John F.; Bashaw, Matthew C.; and Hesselink, Lambertus; "Volume Holographic Storage and Retrieval of Digital Data," *Science,* Vol. 265, August 15, 1994.

Liu, Chong-Yang; Pan, Horng-Long; Fox, Marye Anne; and Bard, Allen J.; "High-Density Nanosecond Charge Trapping in Thin Films of the Photoconductor ZnODEP," *Science*, Vol. 261, August 13, 1993.

Morkoc, H. and Mohammad, S.N., "High Luminosity Blue and Blue-Green Gallium Nitride Light-Emitting Diodes," *Science,* Vol. 267, January 6, 1995.

Neumark, Gertrude; Park, Robert; and Depuydt, James; "Blue-Green Diode Lasers," *Physics Today*, June 1994.

Olson, Gregory; Mocker, Hans; Demma, Nick; and Ross, Jamie Billing; "Coherent CO_2 Laser Communication System with Modulable Retroreflectors," *Applied Optics,* Vol. 34, No. 12, April 20, 1995.

Psaltis, Demetri and Mok, Fai, "Holographic Memories," *Scientific American,* Vol. 273, No. 5, November 1995.

"Real-Time Control of Molecular Beam Epitaxy Offers Major Microelectronic Gains," *Technology Forecasts and Technology Surveys,* Vol. 26, No. 5, May 1994.

Steams, Richard, "Neural Network that Incorporates Direct Optical Imaging," *Applied Optics,* Vol. 34, No. 14, May 10, 1995.

C. SOFTWARE

David Sarnoff Research Center, National Information Display Laboratory Data Sheet, "Wavelet-Based Image Compression."

Rensberger, Boyce, "How Computers Compress Images and Save Time," *The Washington Post,* July 12, 1995.

D. SYSTEM INTEGRATION

Advanced Technology Data Sheet Obtained from Rome Laboratory on World Wide Web.

Buckingham, Michael; Potter, John; and Epifaniot, Chad; "Seeing Underwater with Background Noise," *Scientific American,* Vol. 274, February 1996.

David Sarnoff Research Center, National Information Display Laboratory Data Sheets:

a. "Searching High Resolution Digital Images"
b. "Softcopy Collaboration Prototype"
c. "High Brightness, High Resolution 5 Megapixel Monochrome CRT Display"
d. "Video Exploitation Tools"
e. "Head Mounted Displays."

Department of Computer Science, University of North Carolina at Chapel Hill, Project Summary, March 1995:

a. "Haptic Display Systems Research"
b. "Head-Tracker Research"
c. "Pixel Flow"
d. "Pixel-Planes 5"
e. "The Nanomanipulator"
f. "Ultrasound Visualization Research."

Peterson, I., "Acoustic Snapshots: Images from Noise," *Science News,* Vol. 146, December 10, 1994.

David Sarnoff Research Center, "Real-Time, 3D Micro-Imaging, Visualization and Analysis of Fluid Transport in Microelectromechanical Systems."

(This page is intentionally blank.)

APPENDIX D
GLOSSARY

Appendix D
GLOSSARY

ADONIS	acoustic daylight ocean noise imaging system
ADS	Advanced Distributed Simulation
ANNT	Artificial Neural Network Technology
ARPA	Advanced Research Projects Agency
ASD(C3I)	Assistant Secretary of Defense (Command, Control, Communications and Intelligence)
ASTO	Advanced Systems Technology Office
ATARS	Advanced Tactical Airborne Reconnaissance System
ATM	asynchronous transmission mode
ATR	automatic target recognition
b	bit
BER	bit error rate
BISDN	Broadband Integrated Services Digital Network
BIT	Broadband Information Technology
C2	command and control
C4I	command, control, communications, computers, and intelligence
CAETI	Computer-Assisted Education and Training Initiative
CAW	Certificate Authority Workstation
CCD	charge-coupled device
CCR	Center for Communications Research
CCR	IDA Center for Communications Research
CDL	Common Data Link
CIO	Chief Information Officer
CISS	Center for Information Security Systems
cm	centimeter
COAST	Computer Operations, Audit, and Security Technology
COTS	commercial off-the-shelf
CSCI	Commercial Satellite Communications Initiative
CSTO	Computing Systems Technology Office (ARPA)
DAI	distributed artificial intelligence
DARO	Defense Airborne Reconnaissance Office
DARSC	Defense Airborne Reconnaissance Steering Committee
DGSA	DoD Goal Security Architecture
DIET	Defense Information Enterprise Technologies

DII	Defense Information Infrastructure
DISA	Defense Information Systems Agency
DISN	Defense Information System Network
DISSP	Defense Information Systems Security Program
DIWCC	Defensive Information Warfare Control Center
DMC	Defense Megacenter
DMS	Defense Message System
DNS	Domain Name Server
DOS	Disk Operating System
DRAM	dynamic random access memory
DSO	Defense Sciences Office
DSP	digital signal processor
DSSG	Defense Science Study Group
DTIC	Defense Technical Information Center
DTII	Defense Technology Integration and Infrastructure
DUSD (AT)	Deputy Under Secretary of Defense (Advanced Technology)
EHF	extremely high frequency
EI	Enterprise Integration
EO	electro-optical
ESTO	Electronic Systems Technology Office
FIDDI	Fiber Distributed Digital Interface, Fiber-Optic Digital Data Interchange
FOPEN SAR	foliage penetration synthetic aperture radar
FY	fiscal year
GaN	gallium nitride
Gb	gigabit
GB	gigabyte
Gbps	gigabits per second
GCCS	Global Command and Control System
GCR	group-coded recording
GE	General Electric
GEO	geostationary earth orbit
GPS	Global Positioning System
H/SIP	H-camera sensor improvement program
HAE	high altitude endurance
HIPPI	High Performance Parallel Interface
HPCC	High Performance Computing and Communications
HUMINT	human intelligence
Hz	hertz

IDA	Institute for Defense Analyses
IMINT	imagery intelligence
INE	in-line network encryptor
IR	infrared
ISDN	Integrated Services Digital Network
ISSP	Information Systems Security Program
ITC	Joint Interoperability Test Center
ITO	Information Technology Office
IW	Information Warfare
IW-D	Defense Information Warfare
JIEO	Joint Interoperability and Engineering Organization
JROC	Joint Requirements Oversight Committee
JSC	Joint Spectrum Center
JWCA	Joint Warfighting Capability Assessment
kbps	kilobits per second
km	kilometer
LAN	local area network
LAW	Local Authority Workstation
LED	light-emitting diode
LEO	low earth orbit
M&S	modeling and simulation
MAGIC	Multidimensional Applications and Gigabit Internetwork Consortium
MASINT	measures and signatures intelligence
Mb	megabit
MB	megabyte
MCNC	name of a state-funded microelectronic consortium in North Carolina
MIAG	Modular Integrated Avionics Group
MIME	Multipurpose Internet Mail Extensions
MIMIC	microwave/millimeter wave integrated circuit
MISSI	Multilevel Information Systems Security Initiative
MIT	Massachusetts Institute of Technology
MLS	Multilevel Security
mm	millimeters
MOA	memorandum of agreement
µs	microsecond
ms	millisecond
MSI	multi-spectral imaging
MTO	Maritime Systems Technology Office
mW	milliwatt

NASA	National Aeronautics and Space Administration
NCS	National Communication System
NIDL	National Information Display Laboratory
NIH	National Institute of Health
NIST	National Institute for Science and Technology
nm	nanometer
nm^3	cubic nanometer
NREN	National Research and Education Network
ns	nanosecond
NSA	National Security Agency
NSF	National Science Foundation
OPR	Office of Prime Responsibility
OSF	Open Software Foundation
PC	personal computer
PGM	precision guided munitions
PHIGS+	programmers hierarchical interactive graphics standards
R&D	research and development
RBE	rate-based execution
ROM	read-only memory
RSA	"Public Key" encryption algorithm devised by Rivest, Shamir, and Adelman
SCC	Secure Computing Corporation
SCSI	small computer system interface
SIGINT	signals intelligence
SISTO	Software and Intelligent Systems Technology Office
SMS	softcopy mapping system
SNA	systems network architecture
SNS	Security Network Server
SONET	Synchronous Optical Network
SPARC	Scaleable Processor Architecture
STO	Sensor Technology Office
SYERS	Senior Year Electro-optical Reconnaissance System
TARS	Theater Airborne Reconnaissance System
THz	tera hertz
TOP/IP	Transmission Control Protocol/Internet Protocol
3-D	three dimensional

UAV	unmanned aerial vehicle
UHF	ultra high frequency
USC	University of Southern California
USD(A&T)	Under Secretary of Defense (Acquisition and Technology)
UUV	unmanned undersea vehicle
W3	World Wide Web
WAN	wide area network
WSP	Workstation Security Package
WWW	World Wide Web

(This page is intentionally blank.)

APPENDIX E
DISTRIBUTION LIST FOR IDA DOCUMENT D-1792

Appendix E
DISTRIBUTION LIST
FOR IDA DOCUMENT D-1792

OSD	No. of Copies
Dr. Frank B. Horton, Principal Deputy OASD (C^3I) Pentagon, Room 3E172 Washington, D.C. 20301-3040	1
Captain G. Blackburn, USN Director, Information Warfare OASD (C^3I) Pentagon, Room 3D200 Washington, D.C. 20301-1000	2
Mr. Dennis Nagy Director, CISA OASD (C^3I) Pentagon, Room 1C492 Washington, D.C. 20301-1000	1
Mr. James Bain OASD (C^3I) CISA Pentagon, Room 1C492 Washington, D.C. 20301-1000	1
Mr. Anthony R. Grieco Deputy Director (Electronic Warfare) ODS&TS, OUSD(A&T) Pentagon, Room 2D252 Washington, D.C. 20301-3090	1
Dr. Louis C. Marquet ADUSD (Advanced Development) Pentagon, Room 3D148 Washington, D.C. 20301	1

Mr. Brenton Greene Director, Infrastructure Policy Deputy Under Secretary (Policy) Pentagon, Room 1D464 Washington, D.C. 20301-2200	1
Director, Net Assessment OUSD(P) Pentagon, Room 3A930 Washington, D.C. 20301	1
Ms. Virginia Castor Director, Advanced Technology ODR&E, OUSD(A&T) Pentagon, Room 3D1089 Washington, D.C. 20301	2
Deputy Director for Theater Assessment & Planning ODPA&E Pentagon, Room 2E314 Washington, D.C. 20301	2
Mr. Richard R. Ledesma Deputy Director (Test & Evaluation) ODTSE&E, OUSD(A&T) Pentagon, Room 3D1075 Washington, D.C. 20301	1
Mr. Greg D. Hulcher Special Assistant for Concepts & Plans ODS&TS, OUSD(A&T) Pentagon, Room 3D1038 Washington, D.C. 20301	1
Mr. John V. Ello, Executive Director Defense Science Board Pentagon, Room 3D865 Washington, D.C. 20301	1
Deputy Assistant Secretary for Forces & Resources OASD (SO/LIC) Pentagon, Room 1A674A Washington, D.C. 20301	1

Brig. Gen. Wesley B. Taylor, DASD (Policy & Missions) OASD (SO/LIC) Policy & Missions Pentagon, Room 2B535 Washington, D.C. 20301	1
Dr. G. Menos, Director for Strategic Policy Defense Technology Security Administration 400 Army Navy Drive, Suite 300 Arlington, VA 22202	1

Joint Staff

The Joint Staff
Pentagon, Room 2D874
Washington, D.C. 20301-5000

Attn:	Deputy Director for Intelligence Doctrine, J2P	1
	Chief, IW-Special Technical Operations Division (STOD)	2
	Deputy Director for Politico-Military Affairs (J5)	1
	Deputy Director for Defense-Wide C4I (J61)	1
	Joint Tactical C4I Systems Division (J6J)	1
	Information Warfare Division (J6K)	50
	Director for Operational Plans & Interoperability (J-7)	1
	Director for Force Structure, Resources & Assessment (J-8)	1
	DOM/JSIRMO (Security Review)	3

Joint Commands

Commander-in-Chief (CINC) Pacific Command (PACOM) Attn: J6 Camp Smith, HI 96861-5025	2
Commander-in-Chief (CINC) Central Command (CENTCOM) Attn: J6 MacDill AFB, FL 33608-7001	2

Commander-in-Chief (CINC) European Command (EUCOM) Attn: J6 APO AE, New York, NY 09128	2
Commander-in-Chief (CINC) Atlantic Command (ACOM) Attn: J6 Norfolk, VA 23511	2
Commander-in-Chief (CINC) Special Operations Command (SOCOM) Attn: J6 MacDill AFB, FL 33608-6001	2
Commander-in-Chief (CINC) U.S. Space Command (SPACECOM) Attn: J6 Peterson AFB, CO 80914-5001	2
Commander-in-Chief (CINC) U.S. Strategic Command (STRATCOM) 901 SAC Blvd., STE 2A Attn: J6 Offutt AFB, NE 68113-6000	2
Joint Command and Control Warfare Center 2 Hall Blvd. Kelley AFB, TX 78213-1164	
Attn: Commander	1
Deputy Director for Operations	2

Department of the Army

Assistant Deputy C/S for Force Development Deputy Chief of Staff Operations & Plans Pentagon, Room 2C536 Washington, D.C. 20310	
Attn: Intelligence/EW/C^2CM Division	1
EW Doctrine/C^2CM Office	1
Information Warfare Office	1

Deputy ACSI Office of Assistant Chief of Staff for Intelligence Pentagon, Room 2E466 Washington, D.C. 20310	1
Director, Land Information Warfare (LIWA)-DCSOPS Fort Belvoir, VA 22060	1
Intelligence and Electronic Warfare Directorate Headquarters, U.S. Army Training and Doctrine Command (TRADOC) Fort Monroe, VA 23651-5000	1
C^3 and Intelligence Directorate U.S. Army Combined Arms Center Fort Leavenworth, KS 66027-5000	1
AT SI Commander U.S. Army Intelligence Center and School Fort Huachuca, AZ 85613	1

Department of the Navy

Chief of Naval Operations
Pentagon, Room 4E624
Washington, D.C. 20350-2000

Attn:	DCNO/Plans, Policy and Operations Warfare Policy Branch (N-512) Room 4E531	1
	Director, Space and Electronic Warfare Assistant for EW (N-60G) Room 5A726	1
	Director, Information Warfare Division (N-64) Room 5A678	2
	Director, C2 Systems Division (N-62) Room 5E569	1
	Office of Naval Intelligence (N-2) Room 5C600	1
	Deputy Chief of Naval Operations/Resources Warfare Requirement and Assessments (N-8) Room 4E620	1

Commander 1
Navy Information Warfare Activity (NIWA)
Fort Meade, MD 20755-6000

Center for Naval Analyses (CNA)
4401 Ford Avenue
Alexandria, VA 22302-0268
Attn: Dr. Gary A. Federici 1

Dr. Bruce Wald 1

Commander 1
Fleet Information Warfare Center (FIWC)
Naval Amphibious Base, Little Creek
Norfolk, VA 23521

Department of the Air Force

Office of the Assistant for the Air Force (Acquisition) 1
Director, Electronic and Special Programs (AQL)
Pentagon, Room 5D230
Washington, D.C. 20330

Office of Assistant Secretary of the Air Force (Acquisition) 1
Command, Control and Communication (AFPEO/C^3)
Pentagon, Room 4D287
Washington, D.C. 20330

Office of Deputy Chief of Staff, Plans & Operations
Pentagon, Room 4E1032
Washington, D.C. 20330
Attn: Checkmate Division (AF/XOOC) 1
Room BF938B

Electronic Combat Division (AF/XOFE) 1
Room 4B879

C^2 Combat Integration Requirements Division (AF/XORS) 1
Room 5D285

Assistant Chief of Staff for Command,
Control, Communications and Computers
Pentagon, Room 5B477
Washington, D.C. 20330
Attn: Plans and Policy Division (AF/SCXX) 1
Room 5B315

Assistant Chief of Staff, Intelligence Pentagon, Room 4A932 Washington, D.C. 20330 Attn: Commander Room 4A932	1
Information Warfare (AF/INXI) Room 4B141	1
Director, Programs & Evaluation Pentagon, Room 4E315 Washington, D.C. 20330 Attn: Forces Division (AF/PEF) Room 4C152	1
Deputy Commander for Intelligence/C^3CM Director, Electronic Systems Division (ESD) L.G. Hanscom Field Bedford, MA 01731	1
HQ, Air Combat Command (ACC) Langley AFB, VA 23665 Attn: DR	2
Commander, Air Force Information Warfare Center Kelly AFB, TX 78243-5000 Attn: Commander (CC)	1
Plans (XPXP)	1
Operations (DOOE)	2
Commander Air Intelligence Center (NAIC/CC) Wright-Patterson AFB, OH 45433-5604 Attn: Colonel G. Payton	1
Commandant Air War College/Air University Department of Force Employment Maxwell AFB, AL 36112	1

Other Organizations

Defense Intelligence Agency (DIA) Deputy Director for Intelligence Doctrine Plans, Policy and System Requirements (J2-P) Pentagon, Room 1E880 Washington, D.C. 20301-7400	1
Defense Intelligence Agency-National Military Production Center (PC) Directorate for Military Assessments/DIAC Washington, D.C. 20340-6537	1
Director, National Security Agency Fort Meade, MD 20755-6000	
Attn: Chief, Research and Technology (R2)	1
Deputy Director for Technology and Systems	1
Mr. Robert Ayers, Chief, Information Systems Security Director, Defense Information Security Agency (DISA) 701 S. Courthouse Road Arlington, VA 22204-2199	1
Defense Advanced Research Projects Agency (DARPA) 3701 N. Fairfax Drive Arlington, VA 22203-1714	
Attn: Deputy Director for C^2/Dr. David T. Signori, Jr.	1
Information Technology Office (ITO)/Ms. Teresa Lunt	1
Information Systems Office (ISO)/Dr. Judith A. Daly	1
Commandant Armed Forces Staff College (CAFSC) Norfolk, VA 23511	1
Dr. Stuart Starr MITRE Corporation 7525 Colshire Drive McLean, VA 22102	1
Science Applications International Corporation 1710 Goodridge Drive Attn: Bernie Ziegler McLean, VA 22102	1

Central Intelligence Agency Washington, D.C. 20505 Attn: Director of Intelligence/Office of Information Warfare	1
OSWR	1
NIO/SP, National Intelligence Council Dr. Larry Gershwin, Room 7E47	1
RAND Corporation P.O. Box 2138 Santa Monica, CA 90407-2138	1
National Defense University Fort McNair Washington, D.C. 20319-6000 Attn: President/LTGEN Ervin J. Rokke	1
Dr. John Carabello Information Resources Management College	1
Dr. Fred Giessler School of Information Warfare and Strategy	1
Carnegie-Mellon University Software Engineering Institute (SEI) Attn: Jan Philpot Pittsburgh, PA 15213-3890	1
National Information Display Laboratory David Sarnoff Research Center Princeton, NJ 08543 Attn: Ms. Stephanie Baldwin	1
Mr. Victor Korsun CN 8619	1
Professor Stephanie Forrest Department of Computer Science The University of New Mexico Albuquerque, NM 87131	1

Department of Computer Science University of North Carolina at Chapel Hill Chapel Hill, NC 27599 Attn: Professor Frederick P. Brooks	1
Professor Henry Fuchs	1
Sandia National Laboratory P.O. Box 5800 Albuquerque, NM 87185 Attn: Kevin Killen	1
National Institute of Standards and Technology Computing and Applied Mathematics Laboratory Gaithersburg, MD 20899 Attn: Alfred S. Carasso	1
Santa Fe Institute 1399 Hyde Park Road Santa Fe, NM 87501 Attn: Mr. Thomas Ray	1
Mr. Dan Pirone	1
Los Alamos National Laboratory P.O. Box 1663, Mail Station 5000 Los Alamos, NM 87545 Attn: Information Sciences Division	1
Lawrence Livermore National Laboratory University of California P.O. Box 808 Livermore, CA 94550 Attn: Information Sciences Division	1
Defense Technical Information Center 8725 John J. Kingman Road, Suite 0944 Fort Belvoir, VA 22060-6218	2
Institute for Defense Analyses 1801 N. Beauregard Street Alexandria, VA 22311-1772	50
Total	**216**

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	February 1996	Final

4. TITLE AND SUBTITLE
Information Warfare Technologies: Survey of Selected Civil Sector Activities

5. FUNDING NUMBERS
DASW01 94 C 0054
Task T-I1-1349

6. AUTHOR(S)
W.J. Barlow, R.D. Turner, J.W. Barnett, J.M. Boone, A.E. Brenner, G.L. Brown, J.L. Gerrity, W.T. Mayfield, R.D. Raines, R.S. Ross

7. PERFORMING/ORGANIZATION NAME(S) AND ADDRESS(ES)
INSTITUTE FOR DEFENSE ANALYSES
1801 N. Beauregard Street
Alexandria, VA 22311

8. PERFORMING ORGANIZATION REPORT NUMBER
IDA Document D-1792

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Lt. Col. Steve Spano
Information Warfare Division (J6K)
Joint Staff, Director of C4 Systems
The Pentagon, Room 1C826
Washington, D.C. 20318-6000

Director, FFRDC Programs
2001 N. Beauregard Street
Alexandria, VA 22311

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION/AVAILABILITY STATEMENT
Distribution authorized to U.S. Government agencies and their contractors; Critical Technology; Administrative Operational Use; Specific Authority; 21 June 1996. Other requests must be referred to the Joint Staff.

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 words)*

At the request of the Joint Staff (J6), IDA conducted a survey of emerging technologies in the civil sector that could have long-term influence on DoD Information Warfare activities and initiatives. The survey did not include generic technologies for information systems, or other technologies applicable to sensitive areas that have low visibility in the civil sector. The survey team chose 56 technologies that are briefly described using a specified Joint Staff format that identifies technology strengths and weaknesses, potential applications, compatibility issues, technological risks, and potential limitations. In addition, the document includes an overview of Information Warfare activities in selected Defense Agencies and brief surveys of (1) some trends and implications of technological growth of information technology in the civil sector, and (2) some areas of concern with respected to distributed information systems.

14. SUBJECT TERMS
Information Warfare, Information Warfare technology, information security, information processing concepts, high-performance computing, network technology and distributed information systems, information storage and image representation technology, surveillance concepts, diode lasers, visualization technology, holography, microelectromechanical systems, immunological analogs

15. NUMBER OF PAGES
158

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	SAME AS REPORT

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. Z39-18
298-102

[This page is intentionally left blank.]

[This page is intentionally left blank.]

UNCLASSIFIED / LIMITED