
DEPARTMENT OF DEFENSE

**DEVELOPING CRITICAL
TECHNOLOGIES/SCIENCE &
TECHNOLOGY (DCT/S&T)**

SECTION 10: INFORMATION SYSTEMS TECHNOLOGY



May 2000

**Defense Threat Reduction Agency
Ft. Belvoir, VA**

PREFACE

Developing Critical Technologies/Science & Technology (DCT/S&T) is a product of the Defense Critical Technologies Program (DCTP) process. This process provides a systematic, ongoing assessment and analysis of a wide spectrum of technologies of potential interest to the Department of Defense. DCT/S&T focuses on worldwide government and commercial scientific and technological capabilities that have the potential to significantly enhance or degrade U.S. military capabilities in the future. It includes new and enabling technologies as well as those that can be retrofitted and integrated because of technological advances. It assigns values and parameters to the technologies and covers the worldwide technology spectrum.

DCT/S&T is oriented towards advanced research and development including science and technology. It is developed to be a reference for international cooperative technology programs. A key component is an assessment of worldwide technology capabilities. S&T includes basic research, applied research and advanced technology development.

SECTION 10—INFORMATION TECHNOLOGY

Scope

10.1	Information Communications	10-9
10.2	Information Exchange	10-17
10.3	Information Processing	10-27
10.4	Information Security	10-35
10.5	Information Management and Control	10-61
10.6	Information Systems Facilities	10-67
10.7	Information Sensing	10-75
10.8	Information Visualization and Representation	10-83
10.9	Modeling and Simulation	10-87

Highlights

- Information systems (ISs) will be pervasive in supporting the warfighter in future operations. Advances in technology will allow for capability improvements that will be as natural as normal human physical and mental functions—only enhanced.
- Non-physical conflict, supported by information operations (IOs), will be ongoing and may replace physical conflict in some cases.
- Avoiding the hazards of ill-conceived ISs and their inherent vulnerabilities will be an important consideration for the future warfighter. The enemy of the future will include anyone who deems to cause harm to militarily critical information of ISs.
- ISs will be adapted to the needs and natural style of the individual, allowing the warfighter to concentrate on the battle at hand—be it physical or mental.
- ISs will support the government and military in all phases of military operations, from training to post-conflict analyses, to provide the United States with the most productive and prepared military ever.

OVERVIEW

This section addresses information technologies (ITs) that support IOs—including Information Warfare (INFOWAR)—that are vital to National Security. In the past several decades, reliance on ITs has grown to the point where many vital commercial, government, and military enterprise operations are now critically dependent upon them. Consequently, threats against ISs—and information itself—can place the continuity of critical government, military, and commercial operations at grave risk.

Joint Vision 2010 states that

Improvements in information and systems integration technologies will also significantly impact future military operations by providing decision makers with accurate information in a timely manner. Information technology will improve the ability to see, prioritize, assign, and assess information. The fusion of all-source intelligence with the fluid integration of sensors, platforms, command organizations, and logistic support centers will allow a greater number of operational tasks to be accomplished faster. Advances in

computer processing, precise global positioning, and telecommunications will provide the capability to determine accurate locations of friendly and enemy forces, as well as to collect, process, and distribute relevant data to thousands of locations.

Joint Vision 2010 further states that

. . . forces harnessing the capabilities potentially available from this system of systems will gain dominant battlespace awareness, an interactive “picture” which will yield much more accurate assessments of friendly and enemy operations within the area of interest. Although this will not eliminate the fog of war, dominant battlespace awareness will improve situational awareness, decrease response time, and make the battlespace considerably more transparent to those who achieve it.

Reflecting on this development, the Department of Defense (DoD) has determined that it must be prepared for missions that range from peace to war. These missions include military operations other than war (MOOTW), such as peacekeeping and humanitarian operations, that may be opposed by a wide range of adversaries including state and non-state proponents.

While all editions of the Militarily Critical Technologies List (MCTL) address ITs, the organization and presentation of data have evolved, and the terminology has been refined. To facilitate the establishment of standard terminology, this section adopts DoD Directive (DODD) S-3600.1 definitions and supplements them where DODD S-3600.1 is silent or where additional expository detail is needed. For clarity, the list of definitions in Appendix A presents DODD-S-3600.1- and MCTL-augmented definitions. For consistency, definitions established in this Developing Critical Technologies Section 10 will apply herein and in all future MCT publications.

Section 10 identifies ITs that enable increasingly superior DoD operations or that maintain superior capabilities more affordably. Specifically, these technologies support IOs responsive to the DODD S-3600.1 requirement that

DoD activities shall be organized, trained, equipped, and supported to secure peacetime National Security objectives, deter conflict, protect DoD information and information systems and to shape the information environment. If deterrence fails, Information Operations shall seek to achieve U.S. superiority in times of crisis or conflict.

The range and types of information addressed in this section facilitate the large number and variety of DoD operations specified in DODD S-3600.1. Joint Vision 2010 states that

We must have information superiority: the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary’s ability to do the same.

Because the same IT may be critical to many of the operations defined by DODD S-3600.1, a brief overview of those operations is presented as a context for explanations of why particular ITs are treated.

Figure 10.0-1 illustrates the range of IOs mandated by DODD S-3600.1. The basis for distinguishing, at the highest level, among “pre-hostility” and “post-hostility” operations is that National Security cannot be assured in the absence of appropriate “pre-hostility” DoD operational capabilities. IT requirements are often markedly different in pre- and post-hostility scenarios for secure and covert operations and corresponding capabilities to sustain operations under electronic warfare, physical damage, and chemical and biological and other threat-driven environments.

Explicit reference to the need to support offensive and defensive operations reflects DODD 3600.1’s definitive statement that IOs are actions taken to affect adversary information and ISs while defending one’s own information and ISs. Joint Vision 2010 declares that “information superiority will require both offensive and defensive INFOWAR.” Offensive INFOWAR will degrade or exploit an adversary’s collection or use of information. It will include traditional methods, such as a precision attack to destroy an adversary’s command and control (C2) capability, and non-traditional methods, such as electronic intrusion into an information and control network to convince, confuse, or deceive enemy military decision makers. Defensive INFOWAR to protect our ability to conduct IOs will be one of our biggest future challenges. Traditional defensive INFOWAR operations include physical security measures and encryption. Non-traditional actions will range from antivirus protection to innovative methods of secure data transmission. In addition, increased strategic level programs will be required in this critical area.

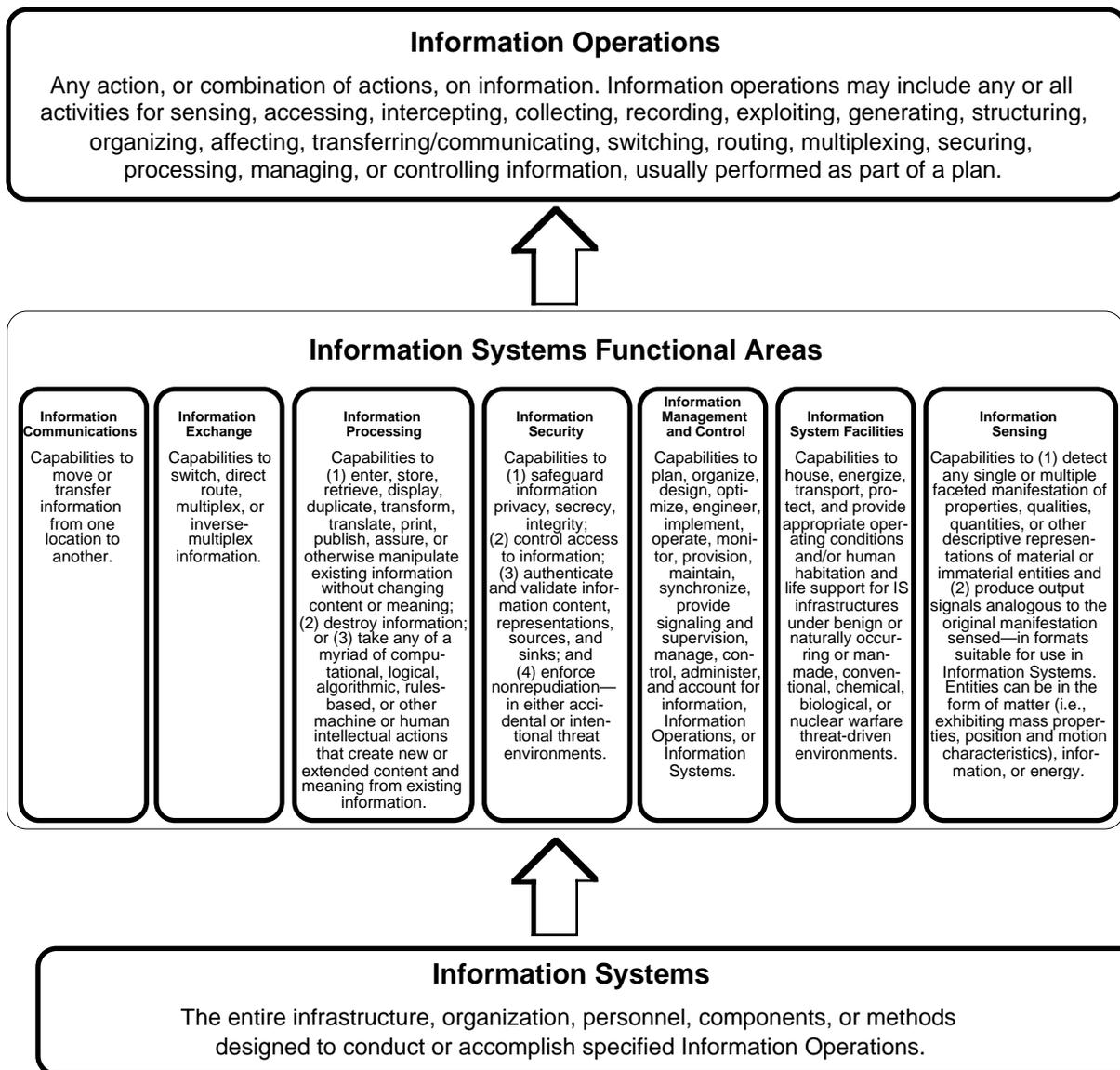


Figure 10.0-1. Information Systems Functional Areas

Historically, a direct relationship has always existed between technologies supporting correlative offensive and defensive military operations. For example, encryption technologies are consummately interrelated to code-breaking technologies and vice versa. Similarly, electronic countermeasure (ECM) techniques essentially may define effective electronic counter-countermeasures (ECCMs). Numerous other examples exist, and, despite U.S. non-aggression policies, National Security makes incumbent the need to pursue, develop, and employ offensive and defensive ITs. Within Developing Critical Technologies Section 10, technologies supporting adverse Information Systems-Affects Operations are presented within sections treating related Functional Areas (FAs). For example, encryption code-breaking technologies are addressed in the Information Security subsection (10.4).

From a National Security perspective, the most familiar IOs are those invoked after active conflict has commenced. Examples of post-hostility IOs include command, control, and intelligence (C2I) operations, ECCMs, psychological warfare, and operations in support of logistics and other military operations associated with conventional and other warfare.

What needs to be emphasized is that post-hostility does not mean post-military conflict alone—nor does it infer target sets limited to physical entities with military-only value. Targets may include manufacturing, transportation, utility, political institutions, and even information itself. Economic, political, and INFOWAR battles can be fought and won or lost in the total absence of any physical military conflict.

Pre-hostility IOs are all other IOs that play direct or indirect roles in U.S. National Security preparedness to conduct any and all forms of authorized offensive and defensive warfare. From a National Security perspective, this IO category includes any IOs that help avert hostilities where possible and ensure victory otherwise. Thus, in accordance with DODD S-3600.1 directives, pre-hostility IOs include all operations needed to prepare for conflict, or, if possible, to prevent escalation to military or other combat. Some pre-hostility operations continue during and after hostilities.

As noted, ITs are used to design and implement ISs, which, in turn, are employed to activate or conduct a wide range of IOs. The enormous range of IOs implied in the definitions gives rise to literally hundreds of categorically different ISs and an almost countless number of identifiable ITs. The selected approach is consistent with the industry-wide practice of specifying large ISs in as many as seven FAs, which are subsets of IS capabilities that accomplish or support specified categories or subsets of IOs (see Fig. 10.0-2). FA requirements are normally, and purposefully, defined and/or specified so that engineers are afforded the greatest possible freedom in making particular hardware or software design choices.

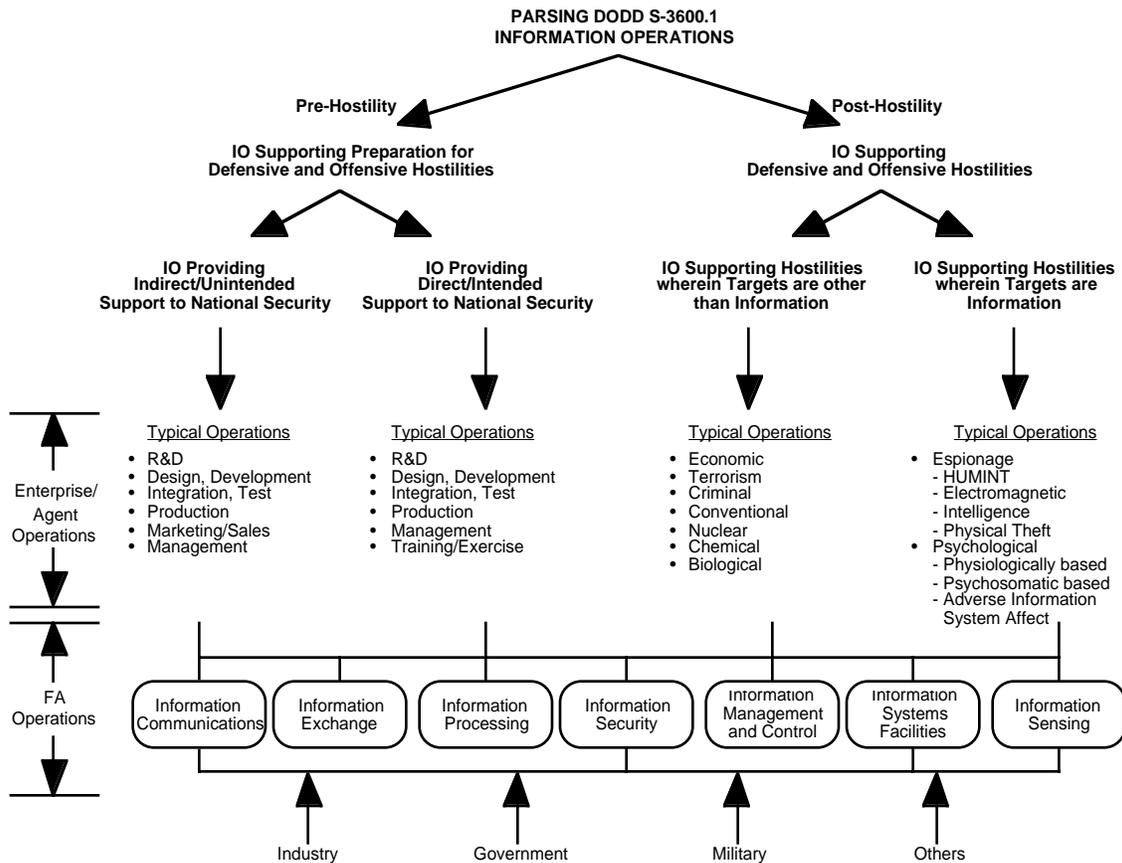


Figure 10.0-2. IO and IS FAs

Given this freedom, vendors in competitive environments are able and motivated to be as creative as possible in proposing IS designs that meet all FA requirements and result in the lowest possible cost and the highest possible operational effectiveness. As an example, procurement specifications written in terms of bandwidth, signal quality, reliability, availability, and other generic communication FA performance parameters leave designers free to make

optimum media and product selections. In this case, vendors attempting to win competitive procurements are highly motivated to propose among metallic or fiber-optic cable, satellite, or terrestrial radio media and product alternatives. These selections not only satisfy all procurement communications FA mission requirements, but also optimize overall “life-cycle” IS cost and operational effectiveness.

Similar assessment and documentation advantages accrue when IT performance levels are stated in terms of generic FA characteristics rather than in terms of extant hardware and software product capabilities. This approach obviates the need to provide updates in response to what may be rapidly evolving performance levels of any particular product or technology type. Thus, updates are only required when:

- Changing mission objectives or operational requirements demand corresponding adjustments to “critical” or “sufficient” IT parameter levels.
- Technological developments advance generic FA performance in ways that enhance the superiority of DoD operations or maintain a superior U.S. capability more affordably.

A separate section is allocated to each of the seven FAs and to each of the two supporting technology areas of “Information Visualization and Representation” and “Modeling and Simulation.” Each section begins with the definition and a narrative description of its IS FA and characteristics. Examples of operations, missions, and objectives and how they relate to cited FA capabilities are included. Technology details and additional expository information are presented in the several data sheets associated with each section.

For presenting ITs, options other than FA decomposition are possible. For instance, information processing (IP) and all the other basic FAs can be subelements of sections treating, for example, Command and Control Systems, Electronic Warfare, any of the other categorical subdivisions, or any new subdivisions envisioned under the rubric of INFOWAR. The problem with this alternative is that unless one sees FA technology developments as being unique to particular IOs or INFOWAR types, the danger exists that the same FA technologies (e.g., “Information Processing”) may be assessed differently by various warfare-operations-specific technical working or author groups, using potentially dissimilar criteria. At best, even if perfectly consistent results are obtained, eliminating the duplication of effort and inefficient use of scarce resources is difficult. Thus, other options for organizing the IT section have been considered but have been determined to be less useful for the purposes of this document.

Although most ITs are treated in this section, some ITs are covered elsewhere. For example, certain information sensor technologies that have traditionally been treated in the “Information Sensors” section are still treated there. Other exceptions made for organizational convenience are noted in the FA sections. Regardless of the section in which ITs are addressed, the definitions and criteria in this section apply.

BACKGROUND

Core Information Technology (IT) Definitions

Because ITs are essential in designing and implementing ISs and because ISs are used to conduct or perform IOs, concise definitions for these word-pairs, as well as for each word taken separately, are crucial. Understanding the need later in this section to define Information Processing, Information Security, Information Communications, Information Encoding/Decoding, Information Translation, and so forth clearly, the “key” word for which unambiguous definition is most needed is “information.” Because “information” appears so frequently in conversation, one might jump to the conclusion that its meaning is universally known and accepted. However, standard and scientific dictionaries not only exhibit large definitional discrepancies, but often employ terms that require exposition.

Although DODD S-3600.1 is silent, the DoD Dictionary of Military Terms defines “information” as:

- Facts, data, or instructions in any medium or form
- The meaning that a human assigns to data by means of the known conventions used in their representation.

As satisfactory as these statements appear, the first definition raises questions about whether “information” and “data” are always equivalent and interchangeable. The second definition employs the term “meaning,” a word that may be as susceptible to subjective interpretation or misinterpretation as is “information.”

To serve as a basis upon which all manner of IOs may be explained herein, “data” are defined as

Representations, such as characters, symbols, or analog quantities, that may or may not explicitly relate to or describe a material or an immaterial entity or process,”

and “information” is defined as

Characteristics, qualities, properties, descriptors, or instructions (elements of information) of any material or immaterial entity or process.

A practical example of how “information” and “data” often differ is to compare the recitation of (1) pairs of numbers and corresponding baseball team-pairs representing yesterday’s game results with (2) the simple recitation of the same numbers, either in pairs or singly, with no reference to any team or inference that the numbers correspond to baseball scores. Most people have little difficulty in grasping the notion that item (1) is a good example of “information,” whereas item (2) is more appropriately categorized as “data.”

Because these two terms are so fundamental and literally serve as a point of departure to everything that follows, it is important, in constructing the preceding definitions, to use words that for most people require no further exposition and to produce explications that apply universally. For the latter point, it is possible, for example, to hold that “information” is only “information” if it is not already known. Certainly, situations exist for which this alternative or specific definition not only applies, but is useful. Importantly, since the notions of “new information” and “old information” are valid, such an alternative definition does not apply universally and is therefore problematic as a basis for the more complex word-pair definitions that are treated throughout the remainder of this section.

DODD S-3600.1 defines Information Operations (IOs) as

Actions taken to affect adversary information and information systems while defending one’s own information and information systems.

In the context of the other DODD S-3600.1 parts cited previously, this definition applies to offensive and defensive operations in missions extending from peace to war. It clearly encompasses all actions taken on information under adversarial conditions. It does not, however, explicitly address an almost countless number of incidences of IOs of a non-adversarial nature. Because many non-adversarial operations are nevertheless vital to National Security, such IOs and their corresponding ITs are considered herein.

Without diminishing the DODD S-3600.1 definition in any way, the following definition is used in the MCTL to describe how ITs, or their amalgamation within complex ISs, are used to support all incidences of IOs. More broadly then,

Information Operations are any action, or combination of actions, on information. Information Operations may include any or all activities for sensing, accessing, intercepting, collecting, recording, exploiting, generating, structuring, organizing, affecting, transferring/communicating, switching, routing, multiplexing, securing, processing, managing, or controlling information, usually performed as part of a plan.

This last “expository” statement is added to provide concrete examples with which many readers may be familiar, thereby clarifying the meaning and intention of the shorter, hopefully universally applicable, basic definition.

DODD S-3600.1, and Joint Publication 6.0 define ISs as

. . . the entire infrastructure, organization, personnel, and components that collect, process, store, transmit, display, disseminate, and act on information.

More recently, Joint Publication 1-02, “DOD Dictionary of Military and Associated Terms,” defines ISs as

The organized collection, processing, transmission, and dissemination of information, in accordance with defined procedures, whether automated or manual. In information warfare, this includes the entire infra-

structure, organization, and components that collect, process, store, transmit, display, disseminate, and act on information.

At first reading, these two definitions do not appear to differ in any substantial way. However, in Joint Publication 1-02, the first sentence defines ISs as “actions” themselves (i.e., “The organized collection, processing, transmission, and dissemination of information”). In contrast, the second sentence represents ISs as the “entire infrastructure, organization, and components” that have the capability to “collect, process, store, transmit, display, disseminate, and act on information.”

To be precise, ISs are physical entities and people that can take—or be in—action, but they can also be in “stand-by” or “stood-down” modes and, therefore, “inactive.” That is, ISs are “capabilities” designed to conduct or accomplish IOs but are not “actions” themselves. Moreover, most complex ISs are designed to support a wide range of IOs. Explained in more detail below, this fact is central to the decision to organize the presentation of ITs in terms of IS FAs, as opposed to categories of either IOs or systems.

Consequently, the DODD S-3600.1 definition for ISs, augmented and shortened as follows, is adopted for use in this document:

Information Systems are the entire infrastructure, organization, personnel, components, or methods designed to conduct or accomplish specified Information Operations.

The augmentation adds to DODD S-3600.1 by explicitly recognizing that ISs are used to conduct or accomplish specified IOs. Note, because the previous IOs definition lists example activities, there is no need to repeat the DODD S-3600.1 list as expository information in the definition of ISs.

Both DODD S-3600.1 and Joint Publication 1-02 are silent on the definition of the word technology. The Export Administration Act of 1979 defines it as

The information and know how (whether in tangible form, such as models, prototypes, drawings, sketches, diagrams, blueprints, or manuals, or in the intangible form, such as training or technical services) that can be used to design, produce, manufacture, utilize, or reconstruct goods, including computer software and technical data, but not the goods themselves.

Since systems engineering and integration (SE&I) are pivotal in complex IS design and deployment, henceforth, technology is defined as

Specific information and know-how necessary for the development, production, and use of a product. This includes engineering and integration for systems (groups of interacting elements acting as a complex whole) as well as individual hardware and software elements necessary to achieve that purpose.

SECTION 10.1—INFORMATION COMMUNICATIONS

Highlights

- Basic electromagnetic communications requirements can be accomplished using a wide variety of commercial-off-the-shelf (COTS) and military-specified products, each with greater or lesser abilities to support military and industrial operations before, during, and after hostilities.
- Industry requirements are typically pursued for economic reasons, whereas military and other government needs are driven by adversarial threats—with affordability playing a lesser-but-still-vital role.
- Systems ostensibly procured for peacetime civilian use can be easily reprogrammed for military applications and can achieve levels of survivability far surpassing lower capacity dedicated military systems.
- Long-distance, beyond-line-of-sight (BLOS) communications provide a payoff from remote reconnaissance and damage assessment, aerial strikes launched from one country on targets in an adversary country, and battlefield C2 within large tactical arenas.

OVERVIEW

The Information Communications (INFO COM) FA is defined as capabilities to move or transfer information from one location to another. Implied in this definition are capabilities to “move or transfer” information in any cognizable form. For instance, information may be in the form of still or moving visual imagery or alphabetic, pictographic-hieroglyphic records. Alternatively, it may be in the form of spoken words, audible alarms, or other acoustic energy. Information Communications FA capabilities are crucial in nearly all information systems; particularly so in command, control, communications, computer and intelligence (C4I) and electronic countermeasure and counter-countermeasure systems.

INFO COM capabilities encompass the means to physically transport information from one location to another or to relay it via electromagnetic, acoustical, or other transmission mechanisms. Figure 10.1-1 shows the range of capabilities that the INFO COM technologies identified in this subsection support.

At least two basic technologies require development to meet future needs for INFO COM:

1. Increasing the total capacity of carriers
2. Increasing the amount of information that can be transmitted per unit time over any given carrier.

High-speed carriers with enormous bandwidths and an exponential growth capability are becoming a commodity, with cost or usage rates becoming insensitive to time or distance charges. Related technologies provide improved availability, reliability, efficiency, and protection from abuse, unauthorized intervention, and capacity saturation.

Physical Transport

Despite technological advancements in modern electromagnetic communications networks and their now nearly global extent, physical delivery remains an important INFO COM mechanism. The persistence and popularity of physical information delivery can be partially attributed to advances in information storage technologies such as compact disks [compact disk-read only memory (CD-ROM)], digital video disks (DVD), videocassette recorder (VCR) video tapes, digital audio tapes, smart cards, and countless others.

Advanced storage technologies that keep physical delivery competitive are discussed in subsection 10.3 Information Processing. Cost and convenience factors continue to be impacted by both storage and networking

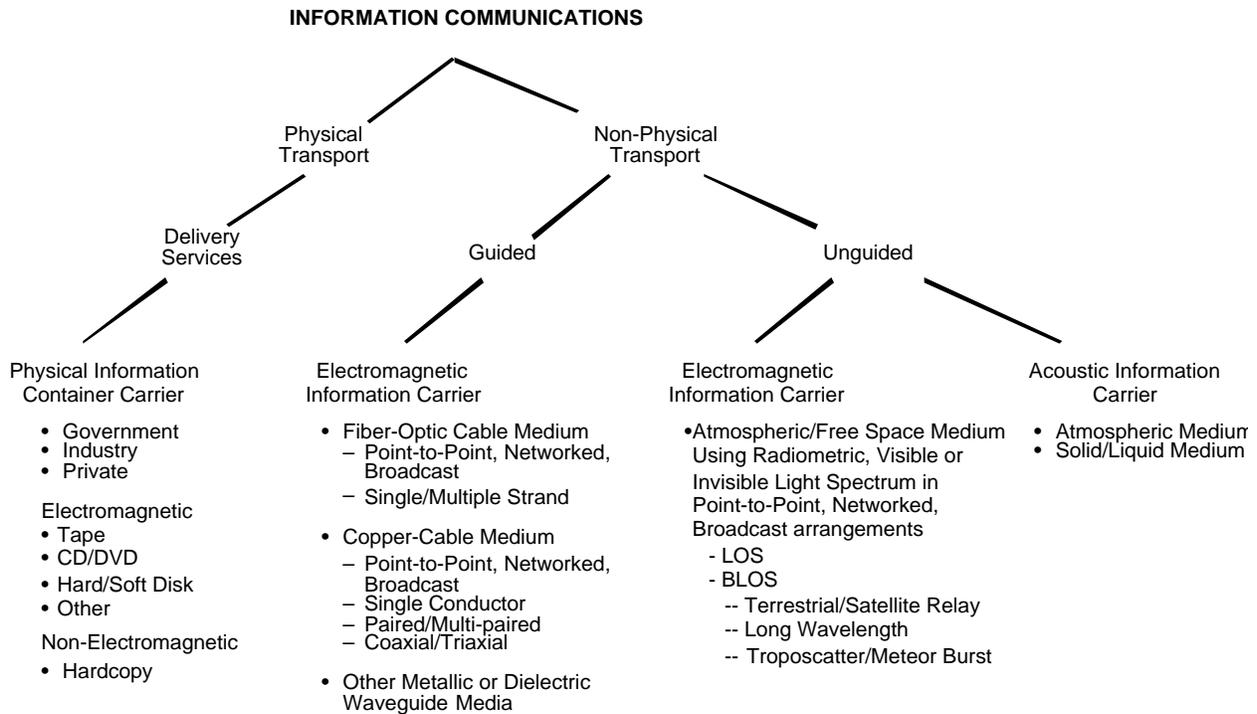


Figure 10.1-1. Taxonomy of Information Communications Technologies

technologies. For example, while most personal computer application software is physically distributed via CD-ROMs, a considerable amount of software is now downloadable via Internet. Similarly, should the cost of viewing video tape recordings (VTRs) via networks drop below the cost of physical distribution and be available for immediate viewing anytime (video-on-demand), the economic case for physical VTR distribution will certainly be diminished.

Another physical delivery tradeoff factor is consumer/user preference. Notwithstanding recent quality enhancements in electronic display technology, many people continue to demand that certain types of information be delivered in hard copy format (newspapers, magazines, books, and so forth). However, even assuming a permanent preference for hard copies, the question arises as to whether personal printers will eventually provide high enough quality and low enough per-page costs to justify printing daily newspapers in offices or kitchens. Along with storage devices that appear to sustain demand for physical information movement or transfer, technologies that may mitigate against such demand (e.g., electronic displays, printers, and associated computer and peripheral equipment) are treated in subsection 10.3.

Non-Physical Transport

As depicted in Fig. 10.1-1, INFO COM via non-physical transport uses either “guided” or “unguided” media. Guided media, including metallic wire cable, fiber-optic cable, and rigid or non-cable-type metallic or dielectric waveguides, constrain electromagnetic waves within boundaries established by their physical construction. Unguided media are those in which boundary effects between “free space” and material substances are absent. The “free space” medium can include a gas or vapor. Unguided media, including the atmosphere and outer-space, support terrestrial and satellite radio and optical transmission. In normal circumstances, liquids constitute an unguided media, usually supporting undersea acoustic communications and sonar systems.

As generally defined, non-physical transport communications systems include transmission facilities, [i.e., the medium (free space, the atmosphere, copper or fiber-optic cable) and electronic equipment located at nodes along the medium]. In this context, equipment amplifies (analog systems) or regenerates (digital systems) signals and provides

termination functions at points where transmission facilities connect to switching or multiplexing systems. Multiplexers (described in subsection 10.2) combine many separate sources of traffic into a single signal to enhance transmission efficiency. In modern designs, transmission termination, switching, multiplexing, and other functions can be “integrated” in a single piece of equipment and, in combination, play major roles in defining network capability, latency, communications services, grade of service, maintenance, reliability, availability, and survivability.

This subsection addresses a wide range of equipment used in local and long-distance communications. Included among “non-integrated” types are simple repeater/amplifiers, channel service units (CSUs), data service units (DSUs), and modems. Modems (MODulator/DEMODulator) are devices that transform digital signals generated by data terminal equipment (DTE) to analog signal formats suitable for transmission through the extensive, worldwide connectivity of public and private, switched and non-switched telephone voice networks. CSUs/DSUs are termination equipment required to connect digital customer premises equipment (CPE) to telecommunications networks and typically provide transmit and control logic, synchronization, and timing recovery across data circuits. Modern, fourth-generation-and-beyond switches and digital cross-connect systems (DCSs) incorporate switching, multiplexing, and line-termination functions. Other examples include satellite, terrestrial microwave, and cable transmit and receive terminals (transceivers), which, in most instances, include multichannel capabilities.

In public cellular or specialized mobile radio (SMR) equipment, basic INFO COM FA capabilities are combined with traditional application-level functions, such as call set-up and take-down dialing, signaling, and so forth; advanced features, such as caller identification (ID); and acoustic and other human interface capabilities. Within cellular or SMR telephones, these application-level functions are typically implemented in software running on embedded microprocessors. In fact, although concepts for mobile cellular telephony existed long ago, practical and commercial viability came only with the appearance of powerful, low-cost, low-power, small, and lightweight microprocessors. Throughout Section 10, “integrated” product technologies are presented in tables of the FA sections to which they are most closely related. For instance, cellular telephone and system technologies, now under discussion, are listed in tables associated with INFO COM FA. Generic ITs, such as general-purpose microprocessors and software, are listed in information processing (IP) FA tables.

LIST OF TECHNOLOGY DATA SHEETS

10.1. INFORMATION COMMUNICATIONS

Communication Links	10-13
Network Access to the End User	10-14
Optical Networks	10-15
Ultra Wide Band (UWB) Communications	10-16

The following developing technologies have been identified, but data sheets are not available at this time:

Alternate Communications Channels
Alternate Routing Algorithms
Backup and Remote Start Technology
Degradation Detection and Degraded Operation Techniques
Disaster Recovery Techniques and Procedures
Dynamic Firewalling Techniques
Intrusion Detection, Correction, and Advisory Techniques
Known and Unknown Virus Detection and Correction Techniques
Message Header Archiving and Message Activity Tracing Techniques
Message Origin and Path Tracing Techniques
Network Activity Analysis and Load Balancing Techniques
Network Activity Sampling and Prediction Algorithms
Network Incident Analysis Techniques
Network Management Techniques
Network Mapping
Network Shutoff or Lock-Up Methods and Procedures
Priority Connectivity Techniques and Protocols
Process and Data Mirroring Techniques
Secure Warning and Correction Notification Procedures
Spoofing Detection and Protection Techniques
Virus Protection Techniques and Secure Notification Procedures

DATA SHEET 10.1. COMMUNICATIONS LINKS

Developing Critical Technology Parameter	Parameters of latency, restoration, and bandwidth availability are of primary importance. Performance concerns are speed, accuracy, and dependability. These can be expressed as link availability, reliability, and efficiency.
Critical Materials	Materials required for fabrication of optical fiber, switches, transceivers, tunable filters, attenuators, and amplifiers as well as high-speed digital circuitry, which is essential for satisfactory operation.
Unique Test, Production, Inspection Equipment	None identified.
Unique Software	Application software.
Major Commercial Applications	Telecommunications services.
Affordability	Leveraging commercial technology will minimize cost.

BACKGROUND

Technologies and methodologies are needed for providing and measuring communications link quality of service (QoS) for wide area networks (WANs) and for local area networks (LANs), including satellite, optical fiber, copper cable, or wireless links. International telecommunications performance standards are needed for use in the emerging Global Information Infrastructure (GII) (Ref. 1).

REFERENCES

1. Neil B. Seitz and Kenneth C. Glossbrenner, "Performance Standards for the GII," *IEEE Communications Magazine*, August 1998, p.116.

DATA SHEET 10.1. NETWORK ACCESS TO THE END USER

Developing Critical Technology Parameter	This technology for connecting the end user to the high-speed fiber network addresses the use of the electromagnetic (EM) spectrum between 24 and 38 GHz, encompassing local multi-channel distribution service (LMDS) and other slots suitable for broadband high-capacity wireless services.
Critical Materials	None identified.
Unique Test, Production, Inspection Equipment	Production of rooftop or window-mounted millimeter-wave radios operating roughly in the 24–38-GHz range.
Unique Software	Software to convert digital bit stream formats among fiber and radio media.
Major Commercial Applications	The commercial potential in the United States is the connection of some 740,000 office buildings (with less than 450 lines per building) to the high-speed fiber backbone. This type of system can run as fast as 200 Mbps.
Affordability	This type of system can cost as little as \$5,000–\$20,000 per facility.

BACKGROUND

This technology uses higher frequencies that are better suited to carrying large volumes of information. It is particularly useful where infrastructure is not currently available. For example, the radio transmission could reach a low earth orbit (LEO) satellite to be relayed to the terrestrial fiber center. It provides more bandwidth than other technologies for connecting the fiber network to the end user.

Internet traffic doubles every few months and is moving the spectrum up to higher frequencies better suited to carrying large volumes of information. The new source of bandwidth frequencies is between 24 and 38 GHz, which encompasses LMDS and other slots suitable for broadband, high-capacity wireless services.

Today, the patch from fiber trunk to end user is done in a variety of more or less unsatisfactory ways:

- **Cable.** Cable is promising in many ways, but chiefly serves residential.
- **Asymmetrical digital subscriber line (ASDL).** ASDL is rolling out relatively slowly and mostly offers less bandwidth than cable.

One of the most promising technologies for end-user access is “up-spectrum wireless.” With connections to the fiber backbone provided by networks of rooftop or window-mounted millimeter wave radios operating roughly in the 24–38-GHz range, these systems can run as fast as 200 Mbps—15 times as fast as any coax or digital subscriber line (DSL) link. In addition, the systems can be installed for \$5,000–\$20,000 per building (figures that are likely to decline further) compared with a typical cost of \$300,000 for a commercial downtown building direct fiber connection.

DATA SHEET 10.1. OPTICAL NETWORKS

Developing Critical Technology Parameter	Fiber speeds of 2.5 Gigabits per second.
Critical Materials	High quality fiber preforms and optical fiber. High performance, non-zero dispersion-shifted (NZDS) fiber is optimized for transmitting multiple wavelength over long distances. Polymeric electro-optic modulators, optochips, can achieve information processing speeds at rates as high as 100 Gigabits per second or 10 times the rate of current electronic devices. Operating voltage is less than one-sixth of current devices- less than a volt.
Unique Test, Production, Inspection Equipment	Production equipment to produce high quality fiber preforms and fiber. Long-wavelength, vertical-cavity, surface-emitting lasers are required to generate longer wavelengths.
Unique Software	Software for connecting self healing optical communication rings and meshes.
Major Commercial Applications	Most of the world wants better, faster and cheaper information transfer. Optical communication networks are being built to fulfill this requirement. Information is transmitted as photons over fiber rather than as electrons over copper making this technology immune to electromagnetic interference and ideal for use in factories having high levels of electromagnetic interference.
Affordability	Cutting-edge optical network technology has dramatically reduced the cost of long-haul communications. The price of bandwidth in competitive areas of the U.S. is now less than one percent of the price in the mid-1980s and is projected to drop an additional 180 fold by 2004. This drop in cost is expected to result in even more bandwidth intensive applications. Operational costs have replaced capital costs during the last two years as the primary network design criteria.

BACKGROUND

Fiber Technology

Technological innovations in optical fiber are overcoming the Internet's delay and bandwidth limitations. Wavelength-division multiplexing (WDM) uses simultaneous multiple channels along a single fiber while channel bandwidths (1–10 Gb/s) are compatible with electronic processing speeds. Experts define three generations in the evolution of high-speed networks. Nodes in the first-generation were connected with copper links and were limited in bandwidth. Second-generation networks replaced the copper with optical fiber and converted optical signals to electronic ones and then electronic signals to optical signals (O-E-O) at each node. Third-generation networks support high-bandwidth and provide a continuous optical connection with data transparency between all nodes.

Research to improve performance and lower cost is ongoing in many areas including tunable lasers, optical code-division multiple access and optical-burst switching. Micro-electromechanical systems (MEMS) optical switches are expected to be used in these implementations. Several companies are developing Petabit (1,000 trillion bit per second) routers to meet projected increases in backbone traffic over the next 4–5 years.

Older fiber has significant Polarization Mode Dispersion (PMD) impairment and special techniques are required to support OC-192 information rates. A widely quoted long-term goal is a 400 nm communications window (nominally 1260–1660 nm) and at a spacing of 50 GHz or less for a potential of 1024 wavelengths by the end of the decade. Ring architecture is currently used to achieve high reliability. Optical switches will probably provide more effective redundancy for future systems using a mesh architecture.

DATA SHEET 10.2. ULTRA WIDE BAND (UWB) COMMUNICATONS

Developing Critical Technology Parameter	Waveform design for anti-jam, low probability of intercept, and bandwidth/power efficiency. < 1 ns impulses, bandwidth > 1 GHz; fractional bandwidth > 25 percent, processing gain > 40 dB.
Critical Materials	Silicon Germanium process integrated circuitry.
Unique Test, Production, Inspection Equipment	None identified.
Unique Software	None identified.
Major Commercial Applications	Automotive, "smart" homes, wireless LANs, large-asset tracking, model control, wireless microphones, radio frequency (RF) ID, and process control.
Affordability	Leveraging commercial technology will minimize cost.

BACKGROUND

An applications demonstration system available in the new term will have the following characteristics:

- 500 ps pulse @ 10 Mpps transmit and receive
- 32 kbps to 2.5 Mbps communications mode
- Radar and ranging modes
- Timing resolution 3 ps
- Timing jitter < 20 ps RMS.

The Federal Communications Commission (FCC) is considering unlicensed, Part 15 compliance and possible interference with GPS and Federal Aviation Administration (FAA) aeronautical communications (Ref. 1).

REFERENCES

1. John Markoff, "FCC Mulls Wider Commercial Use of Radical Radio Technology," *The New York Times*, December 21, 1998, p. C1.

SECTION 10.2—INFORMATION EXCHANGE

Highlights

- Circuit switching, packet switching, and multiplexing capabilities are generally available and installed worldwide.
- Stored program control central office and digital cross-connect switching are key to software defined networks (SDNs) that can be used for survivable communications.
- Fast packet, asynchronous-transfer-mode-based switching and multiplexing support voice, data, graphics, imagery, and video requirements.

OVERVIEW

The Information Exchange (Info Exchange) Functional Area is defined as capabilities to switch, direct, route, multiplex or inverse-multiplex information. Acting together, systems and equipment implementing Information Communications and Exchange capabilities make up telecommunications networks.

Formally, a telecommunications network is a system of interconnected facilities designed to carry traffic that results from a variety of telecommunications services. The network has two different but related aspects. In terms of its physical components, it is a facilities network. In terms of the variety of telecommunications services that it provides, it can support many traffic networks, each representing a particular interconnection of facilities.

Networks consist of nodes and links. Nodes represent switching and multiplexing offices, service provider line termination and other access facilities, user or customer premises, and diverse types of network facility junction points. Links are transmission facilities, and accordingly, traffic is the flow of information within networks, among nodes, over links.

Sections 10.0 and 10.1 cover how all types of guided and unguided media are arranged to provide circuits between telecommunications network nodes and devices. This subsection amplifies earlier references to “*switching*” and “*multiplexing*.” Figure 10.2-1 presents a taxonomy of major Info Com and Info Exch system and equipment capabilities used in combination in many telecommunications networks. At the highest level in the Info Exchange category are functional area capabilities of “switching “ and “multiplexing.”

BACKGROUND

At transmitting nodes, *multiplexing* combines a number of individual communications channels into a common frequency band or a common bit stream for transmission, usually over single circuits. At receiving terminals, “demultiplexing” equipment or processes separate and recover individual channel components of multiplexed signals. Multiplexing makes more efficient use of transmission capacity to achieve low per channel costs.

In theory, the dimensions of *space*, *time*, *frequency* or *code division*, separately or in combination, can be employed in multiplexers to keep individual channel-signals from interfering with each other. Accordingly, these are the dimensions upon which alternative multiplexer designs are based. Although purists would maintain that “space division” may legitimately be used to describe a form of multiplexing, in essence with space division, a separate wire, fiber optic strand or radio frequency link (that is a separate circuit) is assigned to each channel or signal. Practically speaking then, space division multiplexing means no multiplexing at all.

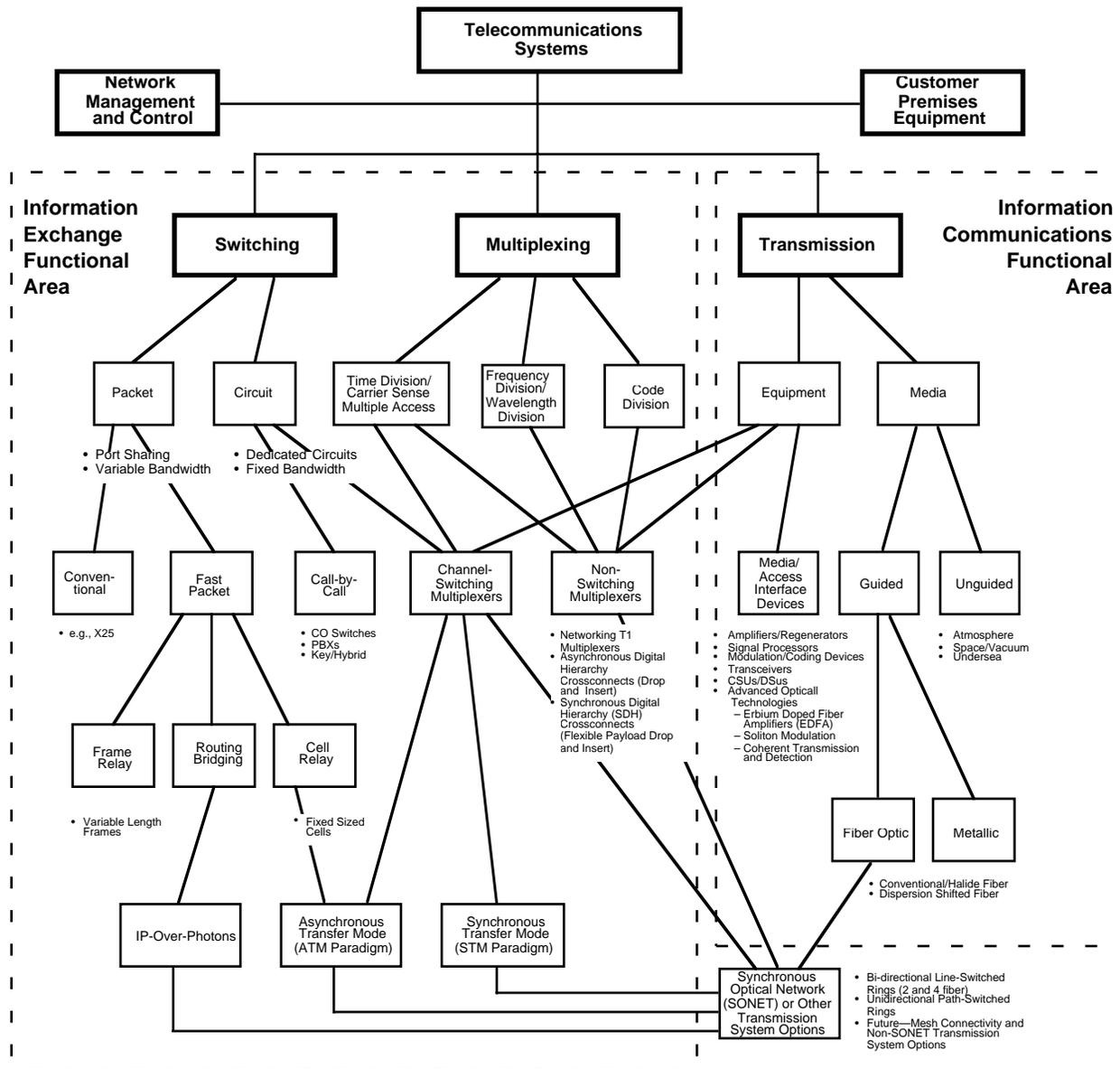


Figure 10.2-1. Taxonomy of INFO EXCH and INFO COM Capabilities

As a consequence, there are three basic multiplexing methods used in telecommunications systems. These are *frequency division multiplexing (FDM)*, *time division multiplexing (TDM)* and *code division multiplexing*, all of which are treated in this subsection. As explained further below, *wavelength division multiplexing (WDM)* is a lightwave version of FDM.

FDM divides the frequency bandwidth (spectrum) of a broadband transmission circuit into subbands, each capable of supporting a single, full-time communications channel on a non-interfering basis with other multiplexed channels. FDM multiplexing is suitable for use with analog carrier transmission systems.

Cable TV is an example where different stations are assigned frequency bands on a single cable medium, and selected by appropriate frequency conversion equipment using either stand-alone “converter boxes” or cable-ready TV set tuners.

In fiber optic transmission, wavelength division multiplexing (WDM) is a form of FDM by which multiple signals of different wavelength are transmitted over the same fiber. Today, a single wavelength channel typically supports 2.5 Gbps of traffic. Eight-channel WDM systems (20 Gbps) are commercially available, with thirty-two-channel systems (an astounding 80 Gbps of capacity on a single fiber strand) currently possible in the laboratory.

In TDM, a transmission facility is shared in time rather than frequency, i.e., signals from several sources share a single circuit or bus by using the circuit or bus in successive “time slots” assigned to each signal source. In the early 1960s “T1-type digital carrier” time division multiplexing was introduced within the old Bell system in which 24 digital voice channels are combined in a single signal.

Subsequently, a five-level Asynchronous Digital Transmission System (ADTS) evolved. The first level, (referred to as Digital Signal-1 or DS-1) supports 24 separate 64 Kbps digital traffic channels (i.e., Digital Signal-0 or DS-0 channels). DS-1 devices generate output signals at the rate of 1.544 Mbps which accounts for the multiple DS-0 input channel, synchronization, and other overhead information. By comparison, deployed DS-4 systems accommodate 4032 digital DS-0 channels and produce 274.176 Mbps signals.

Whereas FDM divides transmission circuit frequency spectrums into subbands, (each supporting single, full-time communications channels on a non-interfering basis), and in TDM, transmission facilities are shared in “time” rather than “frequency,” with *code division multiplexing* (CDM), individual channel-signals are modulated with special, orthogonal coding signals in such a way that multiple signals can be transmitted in the same frequency band and at the same time without interfering with each other.

To recover each transmitted signal individually, receivers must be equipped with an identical version of modulating orthogonal signals. A simple example illustrates CDM’s operating principle. If three signals are represented as S1, S2 and S3, and three modulating signals as C1, C2, and C3, then the output signals from three separate modulators would be: “S1*C1,” “S2*C2,” and “S3*C3,” where using the asterisk means “S1” multiplied by “C1.”

As a consequence, a receiver’s composite input signal is of the form:

$$\text{Receiver input signal} = (S1*C1 + S2*C2 + S3*C3)$$

Now to extract the S1 signal, a receiver-decoder multiplies the receiver input signal by a “local version” of S1’s encoding signal that is “C1.” This produces the following S1 decoder output:

$$\begin{aligned} \text{S1’s decoder output signal} &= (S1*C1 + S2*C2 + S3*C3) * C1 \\ &= (S1*C1*C1) + (S2*C2*C1) + (S3*C3*C1) \\ &= S1 \end{aligned}$$

The orthogonal coding signals C1, C2 and C3 are designed such that the product of different coding signals is “zero”, whereas the cross product of the same encoding and decoding signals is “1.” In practice, approaching this result requires a high degree of synchronism between transmitters and receivers and high quality of coding signals. By high quality codes we mean a set of codes, which when multiplied together, yield a product that is very close to “0” for different codes, and close to “1” for the same code.

In real systems, to approach these ideal results, the bandwidth occupancy of coding signals is often hundreds of times as large as any of the input signals. Thus, the code division multiplexing process is often referred to as a “*spread spectrum*” modulation technique. Whenever wireline or fiber optic receiving equipment, satellites or mobile base stations are designed to receive and handle multiple signals, they are said to exhibit *multiple access* capabilities. Accordingly, linking frequency, time, and code multiplexing to multiple access capabilities produces frequency division multiple access (FDMA), time division multiple access (TDMA), and code division multiple access (CDMA) operations.

Most of the development and refinement of CDMA has taken place to produce military wartime communications with either anti-jam or covert characteristics. As it turns out, because orthogonal coding signals used in CDM/CDMA systems discriminate against all but local versions of themselves, in anti-jam applications they serve to recover desired signal power while minimizing the effects of intentional enemy jamming signals.

Conversely, in covert communications applications, with sufficiently wide spread spectrum bandwidths, it is difficult for enemy receivers that do not possess encoding signals, to even detect that “friendly” transmissions have taken place, much less the ability to surreptitiously listen in on and recover the content of such signals.

Perhaps the most extensive commercial use of CDMA to date is in mobile telephones and base stations. In the United States, designs conforming to EIA/TIA’s IS-95 standard used in Sprint’s PCS service and others employ advanced CDMA and power control approaches to accommodate more users in “fixed” amounts of bandwidth than any other multiple access scheme. Multiplexing and multiple access techniques are typically used in conjunction with, or within, switching mechanisms, addressed next.

Switching systems interconnect transmission facilities at various network locations and route traffic through a network. Switching includes all kinds of related functions, such as signaling, monitoring the status of circuits, translating address to routing instructions, alternate routing, testing circuits for busy conditions, and detecting and recording troubles. The two principal switch-designs are *circuit switching* and *packet switching*.

Treating circuit switching first, most modern circuit-switch matrix designs use time division multiplexing in “time-slot interchange” arrangements. Moreover, nearly all high-capacity circuit-switches provide time division multiplexed outputs at one or more of the DS-“n” levels. Both of these developments affirm close inter-relationships between switching and multiplexing and on-going trends towards even higher levels of equipment and functional integration.

As illustrated in Fig. 10.2-1, all forms of circuit and path-routing SDH/SONET transport network-based switching are implied. In circuit switching, the INFO EXCH functional area encompasses *line* [e.g., central office (CO) telephone exchange call-by-call switching], as well as *channel* switching.

In the past, *channel* switching was implemented manually at technical control centers. In the United States, by the late 1980s, digital cross-connect systems (DCS) began to be installed in 24-channel (“T1,” or more properly, DS-1) group-based Asynchronous Digital Multiplexing and Transmission Systems. Some DCS equipment provides not only channel switching at DS-1 rates (1.544 MBps), but also (1) “drop and insert” multiplexing without “breaking out” each 64 Kbps DS-0 channel, and (2) supergroup (DS-“n”) channel switching. Moreover, these functions are achieved in compact, programmable equipment. Much of this vintage equipment is still in operation and continues to yield enormous economic and functional performance enhancement advantages.

Today, ADTS DCS equipment is being replaced by Synchronous Digital Hierarchy (SDH), International Telecommunications Union (ITU) G-Series or SONET-compliant synchronous byte interleave multiplexer equipment. SDH/SONET-based DCS equipment exhibit all basic asynchronous DCS features.

Beyond basic features, SDH/SONET DCSs capitalize on all of the considerable advantages of synchronous transmission and multiplexing. Among these advantages is the ability to support synchronous payload envelopes (SPEs) that extend “drop and insert” economic and performance advantages across all SDH multiplexing hierarchy levels.

In addition, to enhance survivability and availability, SDH/SONET-based bi-directional line-switched rings (BLSRs) provide reusable bandwidth for more efficient inter-node transport in evenly meshed networks. A meshed network means traffic is more or less evenly distributed among all nodes.

Half the available bandwidth in BLSRs is allocated as a working rate evenly distributed among all nodes rather than being funneled through a few hubbing locations, and the other half is reserved for protection routing. Thus, in an optical carrier, OC-48¹, application, working traffic is placed in the first 24 STS-1² time-slots, with time-slots 25 through 48 serving as a protection facility. In conjunction with ITU Telecommunications Management Network (TMN)-based management functions (or vendor product equivalents), this can result in unparalleled transmission failure recovery-rates, whether failures occur naturally or from intended or collateral enemy attack damage.

1 OC “n”, the “nth” level in an optical carrier multiplexing hierarchy.

2 Synchronous Transport Signal Level 1, equivalent to an OC-1 optical signal.

Network designs using early versions of these techniques have dramatically improved restoration from man-made or natural outages. For example, in 1991 it typically took 120 minutes after a failure to restore 35 DS3 circuits (about 24,000 equivalent DSO (or voice circuits). On July 30, 1996, more than 200,000 circuits were taken out of service when a water department crew bored into a fiber-optic cable in North Carolina. In this case, 92.8 percent of the service was restored in three minutes, nearly ten times the number of circuits in three percent of the time. See subsection 10.5 for a discussion of automated Information Systems Management and Control Functional Area technologies that can lead to this kind of performance in networks used to support military and other missions vital to National Security.

What makes performance improvements of this magnitude possible is not just programmable switching, multiplexing, and computer-based network control technologies, but, as noted in subsection 10.1, the fact that with broadband fiber optic cable and capacity-extending wavelength division multiplexing, for availability and survivability purposes, designers can virtually assume that spare or reserve capacity is “free.” That is, in large commercial or public networks, the 50-percent BLSR “call fill-rate” has no appreciable negative cost or revenue impact.

Another technology category included in the Information Exchange Functional Area is the wide variety of equipment generally described under the rubric of *packet switching*. Unlike circuit switching—which establishes connections on demand and permits the exclusive use of those connections until released—the great advantage of packet switching is that it provides a universal means to allocate network resources to users (devices) *only* when they have information ready to transmit, and makes those resources available to other users or “uses” otherwise. Best of all, it applies to any type or mix of traffic—voice, data video, imagery, etc. Modern data communications networks route traffic among nodes and transmission links using packet switches (the type of packet switch used in the Internet is called a “router”).

A *packet* is a quantity of data that is transmitted and switched as a composite whole. A packet consists of “user data” (for example, some portion of the contents of an electronic mail message) and “control information,” the latter including the “network address” of both originating (sending) and terminating (receiving) equipment. Since the quantity of data packets are able to carry is relatively small, the contents of large messages must be segmented and inserted in multiple packets, in a process referred to as “packet assembly,” often in devices known as packet assembler-disassemblers (PADs).

It is evident that data communications networks require a high degree of compatibility and interoperability among sending and receiving network elements, particularly with respect to physical and logical interfaces and controls. A challenge is presented by different vendor equipment and/or even different models from the same vendor, if they must be interconnected. *Protocols*, that is strict procedures for initiation, maintenance and termination of data communications are defined and invoked to achieve requisite compatibility,

An IP (Internet Protocol) address is an identifier for computers or other devices connected to the Internet. On the Internet, IP addresses mimic the role telephone numbers play in allowing circuit-switches to establish connections between calling and called-party telephone instruments, and IP, in particular, defines packet formats and packet addressing. Thus, IP address information contained in packets is precisely the information packet switches need to route packets from source to destination.

As Fig. 10.2-1 shows, packet switching encompasses conventional and fast packet realizations in both frame and cell relay appearances. Although it is generally appreciated that modern telecommunications systems are increasingly able to integrate voice, data, video, and other services, as observed earlier an even more systemic form of integration is occurring: that is, the integration of switching and multiplexing within single equipment envelopes.

The most recent, and perhaps the most promising manifestation of the integration of switching and multiplexing functions in common equipment, is the Asynchronous Transfer Mode (ATM) digital facility. However, more common so-called local area networks (LANs), LAN routers, bridges, switching and non-switching hubs, and numerous satellite access schemes also provide means for sharing common circuits among multiple traffic channels (multiplexing), and providing either connection-oriented or connection-less switching functions.

A *Local Area Network* (LAN) is a high-speed (typically in the 10 Mbps to 1 Gbps range) data communications system wherein all segments of the transmission medium are in an office or campus environment. LANs are used to connect sets of computers and other devices to one another usually via some shared-medium such as twisted pair, coaxial cable, optical fiber, infrared or radio. On a worldwide basis, the most popular LAN premises data network approach employs *Carrier Sense Multiple Access with Collision Detection* (CSMA/CD), a technique invented in 1972 by recent Massachusetts Institute of Technology graduate Robert Metcalfe, then a Xerox networking specialist. In 1973, he coined the name *Ethernet* which he said comes from "luminiferous ether—the omnipresent passive medium once theorized to carry electromagnetic waves through space."

Ethernet (CSMA/CD) is a contention-based access-control protocol technique by which all devices attached to the network "listen" for transmissions in progress before attempting to transmit themselves and, if two or more begin transmission simultaneously, are able to detect the "collision." In that case each backs off (defers) for a variable period of time (determined by preset "randomizing" algorithms) before again attempting to transmit. Due to the possibility of collisions, LANs operating in CSMA/CD modes typically exhibit a maximum throughput of only about one third of the maximum bit rates that devices and the LAN medium are capable of supporting.

By name and function, LAN components include transceivers, NICs, repeaters, hubs, bridges, switching hubs, routers, and gateways. Today's Ethernet LANs use network interface cards (NICs—printed circuit cards plugged into workstations, PCs, servers or other LAN attached devices), and a transmission medium to which all NICs are connected.

A *hub* is a wiring concentrator used in hierarchical star wiring network topologies. Those directly connected to terminals or other user devices are often referred to as local hubs or concentrators. Central or switching hubs are those at the highest hierarchical level. A certain amount of functional overlap exists among these components. For example, switching hubs possess all the capabilities of non-switching hubs. Moreover, vendors often further classify components in terms of where in the network they are deployed. This gives rise to additional component categories such as backbone switches, workgroup switches, desktop switches and the like. Switching-hubs often eliminate the need to operate in CSMA/CD modes and therefore support information exchange rates equal to the maximum bits rates supported by attached devices and the medium.

Bridges are devices that connect LANs, or LAN segments, providing the means to extend LAN environments in terms of numbers of stations, performance and reliability. *Routers* are devices that connect autonomous networks of like and unlike architectures. Whereas bridges operate transparently to communicating end terminals within a single LAN, routers react only to information addressed to them. Routers, therefore, can interconnect local-to-metropolitan and wide area networks, translating addresses as necessary.

Beyond transceivers, NICs, repeaters, hubs, bridges, switching hubs, routers, and a wire, fiber or electromagnetic medium, (components that establish essential network communications capabilities), most LANs are also equipped with file servers, print servers, application servers, gateway servers, and for larger networks, a network management system.

In addition to the switching and integrated switching-multiplexing equipment described above, equipment assigned to the Information Exchange Functional Area also includes older non-switching "channel bank" and flexible digital time division multiplexers, as well as all forms of analog electronic and photonic multiplexers (e.g., the modern, wavelength-division multiplexers discussed above).

Of course, practical telecommunications networks include a wide variety of modulation, encoding, encrypting, data compression and other information processing capabilities. Implementation of these capabilities may be accomplished in embedded or standalone equipment; may involve analog or digital processing; and may use either software running on general purpose processors or hard-wired logic. Pertinent technologies are found in tables associated with Information Communications, Exchange, Processing and Security subsections of MCT Information Technology documents.

High quality software—controlling signal generation and detection, switching and multiplexing; implementing protocols; and managing communications at device, node, network and service levels—is crucial to day-to-day, crisis, warfare and recovery and reconstitution operations. Methods and techniques for developing, testing and assuring

“trusted,” “virus-proof” and “tamperproof” software and enforcing quality control standards and metrics is treated in subsection 10.3, Information Processing.

LIST OF TECHNOLOGY DATA SHEETS
10.2. INFORMATION EXCHANGE

Network Attached Storage (NAS) 10-24

The following developing technologies have been identified, but data sheets are not available at this time:

Adaptive Video Codes

Adaptive Voice Codes

Amplifying Techniques [Erbium Doped Fiber Amplifier (EDFA) and Raman]

Counter-Cracking Technology

DATA SHEET 10.2. NETWORK ATTACHED STORAGE (NAS)

Developing Critical Technology Parameter	NAS will reduce access time to storage by eliminating the general-purpose server overhead.
Critical Materials	None identified.
Unique Test, Production, Inspection Equipment	Specialized thin clients.
Unique Software	Software or firmware for the specialized thin clients.
Major Commercial Applications	Big databases on the Internet. (For example, mail.com filled up 28 terabytes in 45 days. By comparison, 28 terabytes approximates the total traffic per month on the entire Internet three years ago.) News on demand. Music on demand. Movies on demand.
Affordability	NAS will reduce the cost of storage by replacing comparatively slow complex server operating systems with comparatively fast, specialized thin clients. It also makes the storage more readily available to everyone.

BACKGROUND

The explosion of bandwidth requires a complement of storage. The network has to become a colossal storage system.

Today storage devices, such as disk drives, disk arrays, and Redundant Array of Independent Disk (RAID) technology, are linked to client computers only through various adapters and cable connections:

- Small Computer Systems Interface (SCSI)
- Fiber channel
- Serial Storage Architecture (SSA) (IBM)
- Firewire 1394
- Advanced Technology Attachment (ATA)
- Integrated Drive Electronics (IDE)
- Industry Standard Architecture (ISA).

In addition, wide, fast, ultra, jumbo, turbo, High-Performance Peripheral Interface (HIPPI), and other types and improvements to most of these adapters and cable connections jack up their bandwidth to approximately a gigabit/second.

Linking storage devices directly to the network used to be impractical because the network was too slow to serve as a connector between storage and the rest of the computer. Because of the limits on network speed, storage had to be enslaved to a single computer or server. To get to the storage, the user had to go through the computer—hence, the term “captive” storage. Storage needs were modest and mostly local—modest, in fact, because they were mostly local, comprising only that data likely to be used by the server or its own clients. However, the Web makes this arrangement intolerable. Storage needs are no longer either modest or mostly local, and placing a general-purpose master server between the storage device and the world is extravagant and inconvenient. The new paradigm is that storage is autonomous—thus the term network attached storage, or NAS.

This new paradigm, now commanding between two and five percent of the commercial market, will take it over during the next five years. Storage, long a low-cost peripheral, is expected to account for over 75 percent of all expenditures on computer hardware during this period.

The new system of autonomous storage feeds on a network bandwidth breakout and a traffic transformation. Ethernets are rising to gigabit and even 10-gigabit speeds, while electronic commerce (e-commerce), digital video teleconferencing, video-on-demand, training video, video editing, audio, and other multimedia threaten to swamp all existing storage systems.

In the NAS model, the storage facilities enslaved to a specific server operating system with a specialized file format and expensive proprietary features are gone. Storage is becoming another abundant commodity. The rapidly collapsing price of storage dictates architectures that waste storage and economize on processing and customer time. (Intelligent hierarchical storage systems did just the opposite. Abundance trumps intelligence nearly every time.)

As the network becomes faster than input/output (I/O), the network absorbs I/O. Since I/O is the defining structure of the computer, its dissolution means that the computer disaggregates and becomes a series of peripherals attached to the network.

The simultaneous explosion of bandwidth and storage dictate a similarly massive growth in web caching, a solution that paradigmatically “wastes” these two crucial abundances, while conserving the two great scarcities of telecommunications: the speed of light and the span of life in the form of the customer’s time.

SECTION 10.3—INFORMATION PROCESSING

Highlights

- In view of the rapid pace of commercial technology development, the performance of COTS Information Processing (IP) technology is generally far superior to military standard counterparts.
- COTS IP design, development, test, and evaluation tools facilitate adaptation and upgrade of older military and commercial ISs, delivery systems, and other WMD elements.
- Extraordinary performance growth in ever smaller, lighter, lower power packaging makes the introduction of powerful IP products possible and greatly augments survivable transportable command centers.

OVERVIEW

The IP FA is defined as capabilities to enter, store, retrieve, display, duplicate, transform, translate, print, publish, ensure, or otherwise manipulate existing information without damaging content; to destroy or remove data selectively; or to perform computational, logical, algorithmic, rule-based, and other machine or human emulating intellectual actions that derive new meaning from, or extend the usefulness of, an existing set of information. Figure 10.3-1 is a taxonomy of the major IP system, software, and hardware capabilities required for successful IP operations.

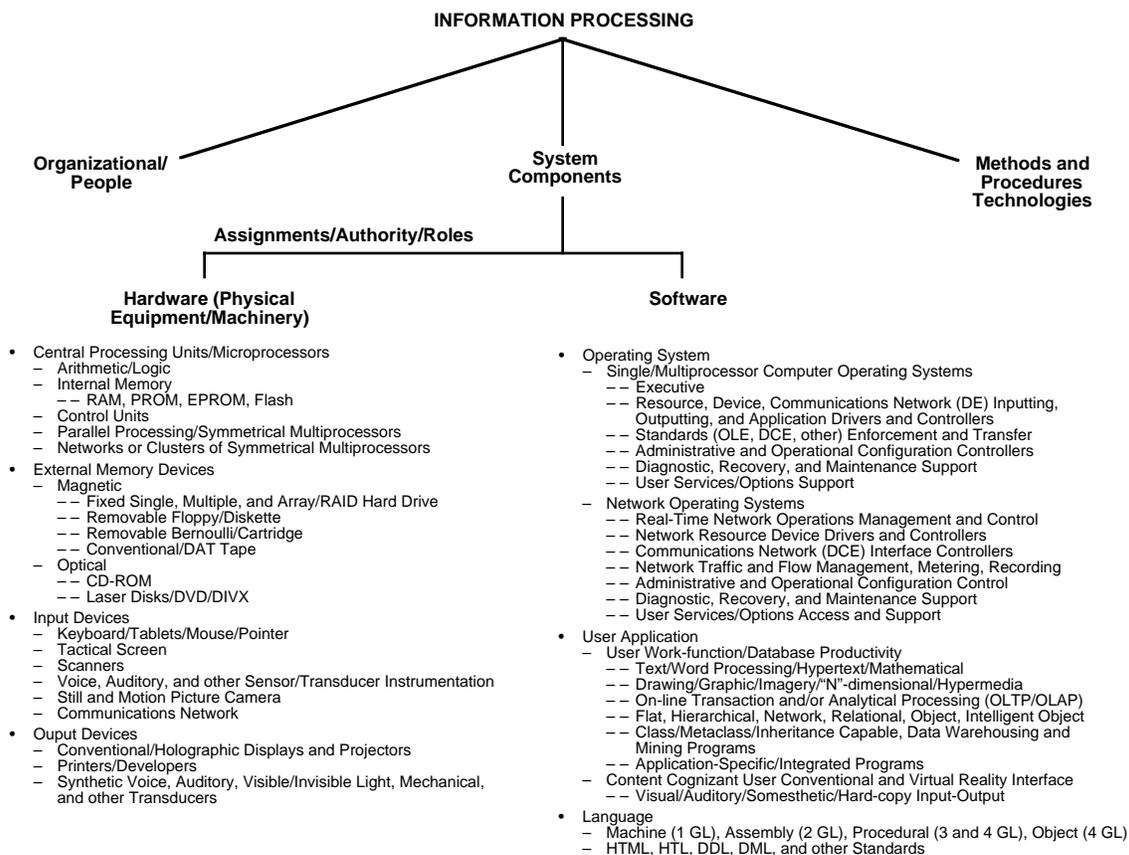


Figure 10.3-1. Taxonomy of IP Infrastructure Capabilities

National Security and commercial organizations need an IP capability that generates timely, reliable, and accurate, data products and services that can be being tailored to each user's needs. Queries must be processed by systems capable of selecting relevant information from among many distributed sources and able to find information immersed in extraordinary quantities of data. After data are found, the system must proceed with a comprehensive analysis and then synthesize or merge analytic results into a coherent projection. Classic systems have been dedicated to processing history archived as events, transactions, or lists. Future systems will use historic data to project probable consequences of action and to present optimal solutions to problems bound by defined constraint parameters. To remain militarily superior and to prevail in future conflicts, sophisticated IP systems must be available for preparation, training, and support of combat forces in the field.

IP trends will be characterized by maturing complexity, searches through huge amounts of data, and a compelling requirement to locate and analyze specific information rapidly. Military applications will access and sort through data stored in public and private domains. A continuous increase in the quantity of data accessible through networks will dwarf rational expectation. Microprocessors—already components of automobiles, ovens, clocks, and credit cards—will become ubiquitous subcomponents of manufactured objects, packaging, and garments. Passive unit processing code (UPC) bar codes will be replaced by active microprocessors that entertain customers, advocate purchases, and record the transaction. The checkout clerk, along with most single-point transaction processing, will disappear. The most mundane interactions of individuals with their surroundings will be noted and recorded by one system or another. The exponential growth in haystack-to-needle ratio will compel the development of agile processing technologies capable of insightfully selecting from among distributed sets of data, correlating and analyzing data swiftly, and presenting results to decision makers at any level of military organization. Disparate data will be gathered from a variety of distributed sources. Most data will be internally organized using different data structures. Some data heaps will lack any recognizable structure or consistent organization. Data mining, use of fuzzy logic³, and verification of data integrity techniques will be managed automatically, and the results will be presented to the user in a quickly understandable form. IS technology will be constantly challenged to produce results *now*.

By increasing the power of automated IP to aid in the rapid conversion of raw data into information, IP systems will augment military capabilities while reducing the number of personnel required to format and enter data queries or to monitor system functions. Speed will provide commanders with the information they need to adapt, modify, or intervene while sufficient time and opportunity still exist.

BACKGROUND

COTS design, development, test and evaluation (T&E) technologies—which are available on the open market—facilitate the adaptation and technology infusion or upgrade of older military and commercial ISs and delivery systems.

Using libraries of generic algorithms, software will adapt and evolve to solve problems without new programming effort. Dynamic applications will be generated and internally quality controlled without having to write additional code. A particular display will be generated, depicted, and then dissolved without having to evaluate or observe (externally) the underlying algorithmic structure. Algorithms that emulate human reasoning processes will be developed and will perform faster (while mastering a greater depth and span of data) than any human brain. Computer algorithms will approach the raw computing capability of the human brain within the next decade.

Neural networks will evolve and emulate the human brain's parallel processing structure. These networks will be able to derive and prove some inductive conclusions. Computerized algorithms will synthesize new knowledge from analytic recognition of previously unnoticed data relationships. Algorithms will be adaptive in the sense of learning from mistakes or through their modification of an initial problem-solving strategy to accommodate an

³ Most computers use logic in which a zero represents False and a one represents True. Fuzzy logic technology allows for degrees of truth by permitting any real number between zero and one to be false, partially true to some degree, or totally true. Internal Fuzzy inference rules vary from the standard predicate calculus and are useful for evaluating incomplete expression terms. "Fuzzy" simply indicates that there is no excluded middle ground.

unstable context presented by a changing set of data. Advanced artificial intelligence (AI)⁴ and a subset of expert systems applications will perform well as decision agents. These programs will appear to behave much as humans when performing duties evaluating an information niche.

Over time, autonomous IP niches, originally developed for narrowly defined purposes, will merge with others that they encounter while actively processing adjacent data turf. Niche-utilities will “discover” one another, interact, and expand the scope of these merged applications. Curiosity behavior, a prelude to intelligence and adaptation, will evolve within AI software applications. Information space, with mathematically defined properties analogous to those defined for a vector space or Hilbert space, will be the domain of transaction and interaction. Boundaries—the edges of computability—will be mathematically derived from those formal properties of information space.

LIST OF TECHNOLOGY DATA SHEETS

10.3. INFORMATION PROCESSING

Data Representation and Visualization	10-31
High Performance Computing (HPC)	10-31
Quantum Information Processing/Communications	10-32

The following developing technologies have been identified, but data sheets are not available at this time:

- Algorithms for Adaptive Learning
 - Analyses Using Dynamic Databases
 - Analytic Recognition of Data Relationships
 - Biological and Psychological Models
 - Boundary Properties Derivation
 - Chaos Theory
 - Commercial-Off-The-Shelf (COTS) Integration
 - Cross Section of Images
 - Data Analysis Techniques
 - Data Into Language of Consumer
 - Data Warehousing and Mining
 - Decision Agents
 - De-conflict Inconsistent Data
 - Distributed Database: Integration, Collaboration, Forward Deployment
 - Dynamic Application Generation
- (Continued on the next page)**

⁴ AI is concerned with emulating human intellectual procedure and behavior through automated models. Humans, with apparent ease, process ambiguous natural language, recognize faces, react to “body language” or tonality of verbal response, and sense of humor or distress. Automating these human behaviors for robotics or computers is an AI challenge.

Flagging Events
Future Projection Techniques
Fuzzy Data Algorithms
Human Interaction
Identification Algorithms for Data Inconsistencies
Impact Analysis (Re-Strike Analysis)
Information Systems, Degraded Capability
Massive Database Filter Algorithms
Monitor System Functions
Neural Networks
Number Theory
Process/Search Tradeoffs of Time and Accuracy Tolerances
Replicated Database
Storage and Retrieval of Information
Total Data Coverage Techniques
Verify Correctness of Data

DATA SHEET 10.3. DATA REPRESENTATION AND VISUALIZATION

Developing Critical Technology Parameter	Size and complexity of the data set. Resolution and response time.
Critical Materials	None identified.
Unique Test, Production, Inspection Equipment	None identified.
Unique Software	Specially designed software that supports direct interaction between the human operator and computer-generated data resources.
Major Commercial Applications	Scientific modeling and enterprise modeling operational control, including computer and telecommunications networks, traffic, financial markets, and so forth.
Affordability	Not determined.

BACKGROUND

The global state of the art in data visualization is growing rapidly because of a combination of growing requirements to deal with very large complex systems (e.g., the Internet, biological systems) and software.

DATA SHEET 10.3. HIGH PERFORMANCE COMPUTING (HPC)

Developing Critical Technology Parameter	Ability to aggregate effective computational throughputs in excess of 1 TeraFLOP.
Critical Materials	None identified.
Unique Test, Production, Inspection Equipment	None identified.
Unique Software	Low latency message passing protocols.
Major Commercial Applications	Pervasive.
Affordability	An explicit goal is to make HPC more accessible.

BACKGROUND

HPC is the single most important enabling technology for modeling and simulation (M&S). Advances in distributed computing networks underlie the development and implementation of the high level architecture (HLA) and the distribution of discrete event (DE) modeling for real-time applications. HPC also supports the calculation of solutions to complex non-linear mathematics, which are used to characterize many physical phenomena, and the generation of realistic environments (visual, auditory, and dynamic) for dynamic training simulations.

Mass market availability of low-cost network switching and powerful microprocessors has resulted in the rapid proliferation and expansion of HPC capabilities. Nearly all the requisite knowledge and software technology required for clustering computers to achieve high performance is in the public domain.

Because of the increased accessibility of the technology, the number and diversity of activities involved in HPC have increased dramatically.

DATA SHEET 10.3. QUANTUM INFORMATION PROCESSING/COMMUNICATIONS

Developing Critical Technology Parameters	Critical parameters cannot be quantified but will be determined by the degree of coherence that can be obtained and the development of effective methods of error correction.
Critical Materials	High-purity materials for quantum devices and specially formulated fluids for molecular and nuclear magnetic resonance quantum computing.
Unique Test, Production, Inspection Equipment	Scanning tunneling and atomic force microscopic equipment for fabrication and inspection of devices. Measurement equipment for determining quantum state, both for testing and as an output mechanism and for implementation of quantum computers.
Unique Software	The inherent ability of the quantum bit (“qubit”) to exploit superposition to encode larger numbers will require development of special algorithms. Error correction algorithms to control decoherence will be crucial to practical implementation of Quantum Information Processing and Communication (QIPC) systems.
Commercial Applications	Driving commercial applications are distant at best. At present, the nearest term prospects appear to be in communications and cryptology.
Affordability	Affordability of access to state-of-the-art computational capability is likely to remain an important consideration. The current movement is toward the concept of centralized HPC resources accessed by what are called “thin clients.” If this paradigm catches hold in the market, pricing strategies for computing will change dramatically, in ways and to an extent that are difficult to project.

BACKGROUND

Quantum information processing (QIP) holds long-term promise for revolutionary advances in computing, communications, and cryptology. Moore’s Law,⁵ which characterizes the rate at which component feature sizes and densities will increase, has proven remarkably durable. However, by the 2000–2015 time frame, projected feature sizes will reach molecular scale. Further advances in computational power will demand some form of computation at the submolecular scale (i.e., atomic scale.)

Quantum computing is perhaps the most promising mechanism yet identified to meet this demand. Since 1994/1995, the amount of work in this area has increased dramatically. This technology is still in its very earliest research phases; however, the amount of the activity and the apparent commitment of the EU and large businesses to support research in this area hold out the possibility of rapid advances.

The time scale for practical implementation of QIP technology is almost certain to lie beyond the 2010 time frame. However, if successful, QIP will enable advances across the full range of military objectives currently envisioned to ensure information superiority. Quantum computing, if successfully implemented, will provide a practical means for rapid code breaking of public key systems. Similarly, quantum communications, in theory, provide a practical counter to this cryptanalytic capability.

⁵ The observation that the logic density of silicon integrated circuits has closely followed the curve (bits per square inch) = $2^{(t - 1962)}$, where t is time in years; that is, the amount of information storable on a given amount of silicon has roughly doubled every year since the technology was invented. This relation, first uttered in 1964 by semiconductor engineer Gordon Moore (who co-founded Intel 4 years later) held until the late 1970s, at which point the doubling period slowed to 18 months.

At present, this work is largely at the stage of basic scientific research into underlying physical phenomena and devices, with some thought being given to algorithm development. The devices themselves are about where the conventional semiconductor transistor was in the late 1950s. The research is widely disseminated and accessible.

Because of the problem of decoherence, quantum computers are likely to be inherently much more susceptible to upset than conventional solid-state computers. At present, it is not possible to predict the extent to which basic isolation measures developed to meet the requirements for general-purpose use will address such vulnerabilities.

Richard Feynman first suggested the notion of a quantum computer in 1982. From the initial idea in 1989 through the early 1990s, David Deutch and Peter Shor of Bell Labs are generally credited with defining the first practical quantum-computing algorithm, a factoring algorithm applicable to decrypting public key information.

Since 1982, rapid progress has taken place in the basic science underlying QIPC. Theoretical analyses indicate that quantum mechanics can be exploited to process and transmit information. Researchers appear confident that a primitive quantum “computer” can be built or that fully secure cryptographic systems can be implemented using quantum effects. Recent breakthroughs in componentry [e.g., the demonstration of elementary quantum logic gates using ion traps, cavity Quantum Electrodynamics (QED), and nuclear magnetic resonance (NMR) technology; the development of error correction and search algorithms; and the quantum teleportation experiments] have helped accelerate quantum computer development. Potentially, QIPC could revolutionize IT. The field is in its earliest phases, and novel ideas and applications will most certainly emerge. While the scientific foundations of QIPC have been reasonably established, technological approaches for practical implementation of QIPC systems do not yet exist.

Preliminary results indicate that quantum computers can perform computations regarded as intractable on any classical computer. Theoretical research indicates that quantum computing has the potential for orders of magnitude increases in the speed at which large numbers can be factored. If this aspect of quantum computing can be made practical, it will have a revolutionary impact on cryptanalysis. All public key cryptosystems, which are used nowadays to protect and to certify electronic documents, will become vulnerable to quantum cryptanalytic attacks. Data security will require different cryptosystems. Quantum cryptography may provide the means for secure communication. Basic research is still necessary in this area to implement quantum logic elements using quantum optics (trapped ions, cavity QED, and so forth). Quantum gates have already been realized in the laboratory. A focused attack on the effects of decoherence on quantum computers is necessary, and quantum error correction codes need to be designed to preserve the quantum information from the deleterious effects of dissipation.

Opinion on the long-term feasibility of quantum computing remains strongly divided. Researchers point to the quality and soundness of the underlying science and argue that the remaining problems are technological—not fundamental—in nature. However, the problem of decoherence (caused by the interaction of the atomic spin state with its external environment) is a daunting problem because it increases exponentially with the number of qubits. For this reason, other scientists predict that systems will be limited to those on the order of 10 qubits.

By comparison with computing, research in quantum communication has been more successful. The partial quantum computers demonstrated secure communication over distances as great as 10 km. Issues of affordability and application requirements will drive future developments. However, implementation of a practical quantum computer capable of decrypting public key cryptography in seconds could dramatically spur demand for quantum encryption.

Among the unanswered questions are:

- Can the problems of scaling up be solved affordably?
- Are there practical solutions to the problem of initializing and maintaining data coherence?
- What classes of problems will QIPC systems be well suited to able to solve?
- In the area of communications, can the quantum phenomena be scaled to practical distances?
- Are quantum repeaters feasible?
- Are there other applications that may lend themselves to smaller scale systems?

To explain what makes quantum computers so different from their classical counterparts, we begin by having a closer look at a basic chunk of information, namely, one bit. From a physical point of view, a bit is a physical system that can be prepared in one of the two different states representing two logical values: no or yes, false or true, or simply 0 or 1. In today's digital computers, the voltage between the plates in a capacitor represents a bit of information: a charged capacitor denotes bit value 1, and an uncharged capacitor denotes bit value 0. One bit of information can be also encoded using two different polarizations of light or two different electronic states of an atom. However, if we choose an atom as a physical bit, quantum mechanics tells us that apart from the two distinct electronic states, the atom can also be prepared in a coherent superposition of the two states. This means that the atom is both in state 0 and state 1. No equivalent of this superposition exists in the classical world. It is a purely quantum mechanical phenomenon.

Because of superposition, a quantum register composed of three qubits can encode eight numbers in a quantum superposition. Storage capacity increases exponentially with the number of qubits. Thus, L qubits can store 2^L numbers at once. Once the register is prepared in a superposition of different numbers, we can perform operations on all of them. In theory, suitably tuned laser pulses could be used to arrange the atomic electronic states and to manipulate initial superpositions of encoded numbers into different values. The result would allow a massively parallel computation. A quantum computer might perform in one computational step the same mathematical operation on 2^L different input numbers encoded in coherent superpositions of L qubits. Thus, a quantum computer offers enormous potential gain in both speed and memory capacity,

With regard to communications, theoretical results indicate that two-state systems can carry more than one bit of information if quantum entanglement is employed. This and related phenomena (e.g., quantum teleportation) may improve channel capacity and optimize data-compression schemes. As noted elsewhere, greater initial success has been realized in the area of quantum communications, and this is where the heaviest industrial participation appears to be focused.

SECTION 10.4—INFORMATION SECURITY

Highlights

- Information Security (INFOSEC) cryptologic technologies are an increasingly important set of present and future militarily critical technologies required to maintain the confidentiality, integrity, and availability of information within processing or storage nodes and while en route over communications networks.
- Strong personnel, facility, equipment, standardization, training, and T&E security programs as well as defensive IOs and Operation Security (OPSEC) are required.
- Commercial INFOSEC products are available on world markets, with capabilities deemed adequate for military IOs in COTS versions, many of which can be customized for more sophisticated command, control, communications, computers, and intelligence for the warrior (C4IFTW) applications.
- Open market-based INFOSEC R&D in cryptology, computers, software and key management architectures, related standards, and the functional specification of key management infrastructures and protocols are required for U.S. forces to maintain information dominance.
- As commercial and government INFOSEC technologies advance, the INFOSEC products necessary to maintain the existing superior U.S. INFOSEC capabilities will become more affordable.

OVERVIEW

The INFOSEC FA is defined as capabilities to safeguard information privacy, secrecy, and integrity; to control access to information; to authenticate and validate information content, representations, sources, and sinks; and to enforce non-repudiation—in either natural or manmade threat environments. INFOSEC FA capabilities are countermeasures intended to prevent or circumvent information loss, degradation, compromise, or improper use. This may occur within systems hardware or software, within communications or physical transport systems, or directly among people.

The range of possible threats is broad. At the highest level, INFOSEC threats are either natural or manmade. Natural threats include earthquakes, floods, sunspots, and phenomenological electromagnetic events. Manmade threats can occur because of actions or events caused by people or other system components internal to an IS (insider/inside threats). Alternatively, manmade threats can involve external actions or events (outsider/outside threats). At the next lower level, manmade threats can be subdivided into either deliberate-intentional or accidental-failure categories.

According to analyses of documented information-loss cases conducted over the past decade, about three percent are attributed to natural causes, and 97 percent are attributed to manmade causes. Of losses attributable to manmade threats, about 92 percent are traceable to insider/inside threats, and six percent are traceable to outsider/outside actions or events. Of the 92 percent of cases resulting from insider/inside threats, about 83 percent occurred because of unpremeditated personnel or system failures (e.g., errors in judgment or performance; hardware or software failures). Insider actions, intentional sabotage, theft, or compromise attacks caused the other three percent. Of the six percent of cases resulting from outsider/outside threats, about three percent occurred because of unintentional personnel or system failures (e.g., power outages and plane crashes). Outsider, intentional sabotage, theft, or compromise attacks caused the other three percent.

Few commercial, government, or military information systems do not employ technologies cited in this INFOSEC subsection. Moreover, within military IS, a nearly universal requirement exists for INFOSEC system protection to conceal intent during the planning, preparation, and operational phases of military operations.

Figure 10.4-1 is a taxonomy of major system, equipment, process, and procedural defensive or countermeasures and offensive or counter-countermeasures INFOSEC technology capabilities. In the figure, INFOSEC capabilities are depicted under five categories that are related but largely non-overlapping functionally.

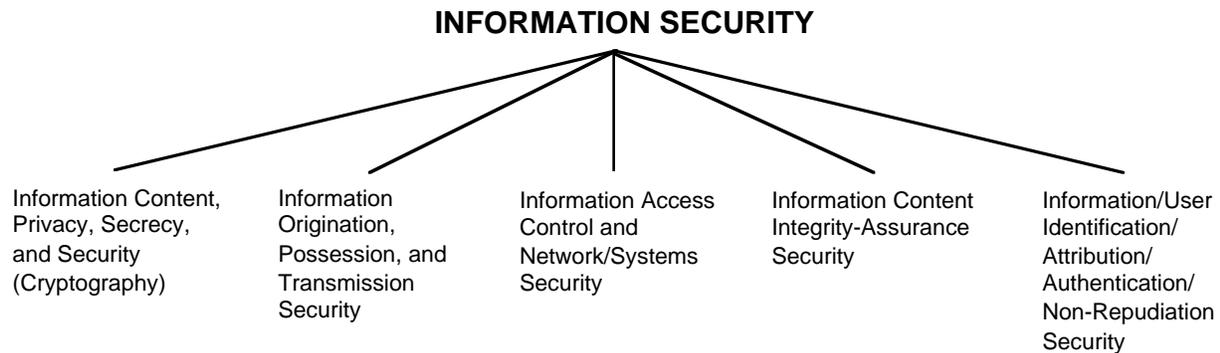


Figure 10.4-1. INFOSEC Applications

The “Information Content, Privacy, Secrecy, and Security (Cryptography)” category (see Table 10.4-1) lists all manner of techniques to prevent unauthorized apprehension of information’s substantive meaning or significance as conveyed by its content. Included among various technologies safeguarding the content of information in electromagnetic form—whether it is contained within electronic or photonic devices or en route over suitable media—are encryption, scrambling, and concealment, using steganographic or secure modulation schemes. Physical protection of information content is accomplished by using protected red-enclaves, protected wire distribution facilities, diplomatic pouch and other secure physical transport, and the manual application of various encoding and steganographic mechanisms.

Table 10.4-1. Information Content, Privacy, Secrecy, and Security (Cryptography)

Offensive Counter-Countermeasures	
<i>Communications Intelligence (COMINT)</i> <ul style="list-style-type: none"> • Cryptanalytic attacks <ul style="list-style-type: none"> – Known plain text – Chosen plain text – Chosen cipher text – Brute force 	<ul style="list-style-type: none"> – Protocol – Massively parallel/symmetrical multi-processors – “Black-bag” enhanced • Escrowed encryption • Time/frequency analysis synthesis • Image processing/pattern recognition
Defensive Counter-Countermeasures	
<i>Electromagnetic</i> <ul style="list-style-type: none"> • Encryption/decryption <ul style="list-style-type: none"> – Symmetric-key (secret-key) <ul style="list-style-type: none"> -- Block and stream ciphers -- Substitution and transposition ciphers -- Digital signatures and hash functions -- Authentication and identification -- One-time pads -- Operational codes – Asymmetric-key (public-key) <ul style="list-style-type: none"> -- Factorization -- Discrete log -- Elliptic curve – Mixed symmetric-asymmetric (hybrid) 	<ul style="list-style-type: none"> • Static/dynamic scrambling <ul style="list-style-type: none"> – Frequency domain – Time domain – Hybrids • Secure non-linear pseudo-noise modulation • Steganography <i>Physical</i> <ul style="list-style-type: none"> • Protected red-enclave • Protected wire distribution • Diplomatic pouch and other protected physical transport • Manual hardcopy encoding/steganography

The “Information Origination, Possession, and Transmission Security” category (see Table 10.4-2) includes technologies to conceal the origination, storage, existence, or possession of information at any node or location; to conceal the fact that information is, or has been, “transmitted” from one location to another; and to ensure successful transmission under natural or manmade threats. In conjunction with appropriate electromagnetic, acoustic, and visual emissions control technologies (e.g., TEMPEST-protected structures), the established OPSEC procedures (e.g., the creation of “black” or compartmented programs and facilities) comprise the principal mechanisms for keeping secret the generation, storage, use, or existence of sensitive information.

Table 10.4-2. Information Origination, Possession, and Transmission Security

Offensive Counter-Countermeasures	
<p><i>Communications Transmission Concealment</i></p> <ul style="list-style-type: none"> • Unguided <ul style="list-style-type: none"> – Electronic signals intelligence/exploitation <ul style="list-style-type: none"> -- Radio fingerprinting -- Enhanced radiometric detection – Spoofing/communications deception • Guided <ul style="list-style-type: none"> – Authorized/ clandestine wiretapping 	<p><i>Communications Transmission Assurance</i></p> <ul style="list-style-type: none"> • Unguided <ul style="list-style-type: none"> – Jamming, spoofing, repeating <ul style="list-style-type: none"> -- Radio fingerprinting • Guided <ul style="list-style-type: none"> – Transmission facility sabotage <p><i>Counter Operations Security</i></p> <ul style="list-style-type: none"> • Operations Intelligence
Defensive Counter-Countermeasures	
<p><i>Communications Transmission Concealment</i></p> <ul style="list-style-type: none"> • Unguided <ul style="list-style-type: none"> – Low probability of intercept – Spread spectrum – Low power/duty cycle – Hybrids <ul style="list-style-type: none"> – Steerable/narrowbeam antennas – Facility/equipment TEMPEST protection • Guided <ul style="list-style-type: none"> – Protected wire distribution – Fiber-optic/metallic cable <p><i>Steganographic Decoy Transmission</i></p> <p><i>Transmission Assurance</i></p> <ul style="list-style-type: none"> • Unguided <ul style="list-style-type: none"> – Survivable/anti-jam communications – Spread spectrum – High power – Steerable/narrowbeam antennas 	<ul style="list-style-type: none"> • Unguided/guided <ul style="list-style-type: none"> – High survivability and availability – Redundant multimedia networks – High reliability fault tolerant designs – Radiation, EMP/HEMP/SGEMP hardened <p><i>Operations Security</i></p> <ul style="list-style-type: none"> • Identifying, controlling, and protecting evidence of the planning and execution of sensitive activities • Actions to conceal information origination and/or existence of <ul style="list-style-type: none"> – Secure compartmented programs – Special access programs – Information, facilities, and equipment

In the unguided electromagnetic signals domain, “transmission concealment or hiding” is typically achieved by using spread spectrum. The transmission of signals is concealed in guided electromagnetic communications systems by using emission-suppressing “protected wire distribution” facilities employing either fiber or metallic cable.

Again, in the unguided electromagnetic signals domain, “transmission assurance” relies on the use of spread spectrum, high-power, steerable, narrow beam antennas, or hybrids of these technologies to achieve robust anti-jam, anti-spoofing communications capabilities. High-transmission survivability and availability are attained through the use of redundant media (e.g., multiple satellite, terrestrial radio, and wireline communications); high reliability and

fault-tolerant, fault-detection, and fault-correction designs; and, when required, radiation, electromagnetic pulse (EMP)/high altitude electromagnetic pulse (HEMP)/system generated electromagnetic pulse (SGEMP) hardening.

Although the transmission concealment and assurance technologies just described can be properly assigned to the INFOSEC FA, they also qualify as INFO COM technologies and, for organizational reasons, are listed in INFO COM tables.

Technologies providing “Information Access Control and Network/Systems Security” (see Table 10.4-3) again encompass both electromagnetic and physical protection measures. Unlike previously discussed encryption technologies that attempt to conceal content, the information access control and network/systems security technologies protect information by denying unauthorized access to sources of information or system/network resources.

Table 10.4-3. Information Access Control and Network/Systems Security

Offensive Counter-Countermeasures	
<p><i>Espionage</i></p> <ul style="list-style-type: none"> • Electromagnetic <ul style="list-style-type: none"> – Transmission interception – Unguided (terrestrial/satellite surveillance) – Guided (e.g., wiretapping) – TEMPEST emission surveillance – Storage media/equipment theft – Escrowed encryption – Network, switch, server, router, multiplexer attacks – Jamming, spoofing, repeating <ul style="list-style-type: none"> -- Public key factoring attacks -- Automated password/war dialer attacks 	<ul style="list-style-type: none"> • Physical hardcopy theft/duplication • Acoustic and visible and Invisible – lightwave activity surveillance <p><i>Systems Influence</i></p> <ul style="list-style-type: none"> • System, network, product hardware and software <ul style="list-style-type: none"> – Operating system, executive, and application software – ASIC • System, network, product hardware and software operational phase sabotage <ul style="list-style-type: none"> – Remote/networked virus, spoofing, spamming attacks – On-premises hardware and software attacks
Defensive Counter-Countermeasures	
<p><i>Electromagnetic</i></p> <ul style="list-style-type: none"> • Digital certification and authorities • Key management <ul style="list-style-type: none"> – Key backup and recovery – Key updating and revocation – Key registry and distribution • Network security <ul style="list-style-type: none"> – Multilevel security – Firewalls, passwords, smart cards – Encrypted management/control and common channel signaling • Systems security <ul style="list-style-type: none"> – Trusted IS designs – Defect/virus/trapdoor free software – Defect/bug free hardware • Intellectual property theft-deterrence/secure container/usage metering • Threat/attack detection, response, prevention 	<p><i>Steganographic Decoy Transmission</i></p> <p><i>Transmission Assurance</i></p> <ul style="list-style-type: none"> • Unguided <ul style="list-style-type: none"> – Intrusion-resistant fiber-optic cable – Metallic cable shielding and time domain reflectometry – Transaction (e.g., long-on/penetration attempt) monitoring and auditing – Operational detection and neutralization of software (e.g., virus, Trojan Horse, spoofing) and hardware sabotage attacks <p><i>Physical</i></p> <ul style="list-style-type: none"> • Tamper-proof packaging • Electronic/physical locks • Protected red enclaves

In the electromagnetic class, techniques for limiting access include digital certificate, certificate authority, and associated key management technologies. Trusted IS designs include an extensive array of system/network security technologies. These technologies range from sophisticated techniques to ensure defect- and bug-free software and hardware, multilevel security, firewalls, and so forth, to less complex password and management/control and common channel signaling encryption.

In another aspect of access control, emerging technologies prevent outright theft of intellectual property and yet permit IS marketing and sales distribution using “secure container and metering” capabilities. In addition, a major facet of electromagnetic information access control is the detection, neutralization, and prevention of successful unauthorized interception and infiltration attempts. At the logical network and application level, pertinent technologies include access-seeking transaction monitoring and auditing and the detection and removal of software (virus, Trojan Horse, and spoofing) and hardware sabotage attacks.

Finally, in the physical access control arena, tamper-proof packaging is critical when equipment containing sensitive information must either be given to—or may be stolen by—potential adversaries. Other physical access protection approaches include protected red enclave and simpler electronic or mechanical locks. The wide-ranging variety of room-building-campus perimeter access control, intrusion detection, and alarm capabilities—when used to safeguard information—merits inclusion among the technologies identified in this subsection. However, for organizational reasons, these technologies are discussed in subsection 10.6.

Technologies providing “Information Content Integrity-Assurance Security” (see Table 10.4-4) apply only to information that, at least at some point, exists in electromagnetic form. These technologies are designed to detect and, if possible, mitigate naturally occurring errors or intentionally induced manmade alteration of the information content en route between senders and receivers. Such errors often occur because of natural background noise and intentional or unintentional interference that degrades communications channel quality. Information coding technologies that either detect—or both detect and correct—errors are commonly used in data communications to circumvent or at least alert users that received information may be corrupted or invalid.

Table 10.4-4. Information Content Integrity-Assurance Security

Offensive Counter-Countermeasures	
<p><i>Electromagnetic Record Security Counter-Countermeasures</i></p> <ul style="list-style-type: none"> • Unguided <ul style="list-style-type: none"> – Jamming/repeated-signal transmission denial attacks – Deceptive signal transmission attacks • Unguided/guided <ul style="list-style-type: none"> – Random/deterministic content manipulation – Transmission denial attacks 	<p><i>Information/Knowledge Accuracy Counter-Countermeasures</i></p> <ul style="list-style-type: none"> • Psychological operations <ul style="list-style-type: none"> – Philosophically based – Physiologically based – Psychosomatically based • Industrial/financial-economic/scientific disinformation operations • Government/political disinformation operations • Military situation disinformation operations
Defensive Counter-Countermeasures	
<p><i>Electromagnetic Record Assurance</i></p> <ul style="list-style-type: none"> • Error detection and correcting codes • Secure hash functions <p><i>Information/Knowledge Accuracy Assurance</i></p> <ul style="list-style-type: none"> • Psychological operations detection/countermeasures <ul style="list-style-type: none"> – Philosophically based 	<ul style="list-style-type: none"> – Physiologically based – Psychosomatically based • Industrial/financial-economic/scientific disinformation operations • Government/political disinformation operations • Military situation disinformation operations

Information operated on by hash functions produces “message digests.” Because two messages can hash to the same digest, secure reception of a message digest along with the message itself provides means to ensure received-message integrity. Since messages with errors introduced during transmission, whether unintended or induced, produce different digests, comparing locally generated and transmitted digest yields a “foolproof” method for detecting corrupted or altered content.

To be effective, the technologies for Information/User Identification/Attribution/Authentication/Non-repudiation Security (see Table 10.4-5) are typically employed in unison with those of other categories. For example, recipients in most INFOSEC environments require assurance that messages have not been surreptitiously intercepted

and plain text-content revealed (which demands effective encryption technologies), assurance that message content has not been altered (which demands effective hash functionality), and some means to authenticate and validate that “particular” messages were sent or approved by some authority and source that can be positively identified.

Table 10.4-5. Information/User Identification/Attribution/Authentication/Non-Repudiation Security

Offensive Counter-Countermeasures	
<i>Information Attribution</i> <ul style="list-style-type: none"> • Electromagnetic <ul style="list-style-type: none"> – Counterfeit source/sink/date/container/file location/time-to-user ID attacks • Physical <ul style="list-style-type: none"> – Counterfeit hardcopy substitution/delivery 	<i>User Identification</i> <ul style="list-style-type: none"> • Counterfeit badges/cards • Unauthorized use of user-unique information
Defensive Counter-Countermeasures	
<i>User Identification</i> <ul style="list-style-type: none"> • Badges/cards/personal identification numbers (PINs) • Smart cards • Biometrics <ul style="list-style-type: none"> – Thermograms – Hand or eye scanning – Voice printing – Keyboard rhythm – Fingerprint – Signature dynamics 	<ul style="list-style-type: none"> • Digital certification <ul style="list-style-type: none"> – Digital signature algorithms and techniques <i>Information Attribution</i> <ul style="list-style-type: none"> • Electromagnetic <ul style="list-style-type: none"> – Source/sink/date/container/file location/time-to-user ID correlation • Physical <ul style="list-style-type: none"> – Registered/certified mail – Diplomatic pouch/carrier/commercially validated hand delivery

To satisfy the third requirement (i.e., that messages were sent or approved by some authority and source that can be positively identified), correlation of positive sender identification and validation with error free and content-assured-received secure messages is needed. Capabilities supporting user ID include thermogram, hand or eye scanning, voice printing, keyboard rhythm, fingerprint, signature dynamics, and other biometric technologies; a broader set of digital-certificate-based techniques; and simpler PINs and individual-unique data (e.g., a mother’s maiden name or birthday). With third-party Digital Certificate Authorities, these technologies also support objective non-repudiation capabilities.

LIST OF TECHNOLOGY DATA SHEETS
10.4. INFORMATION SECURITY

Cryptology	10-42
Distributed Key Generation	10-43
Electronic Cash (e-cash) Transfer System	10-44
Elliptic Curve System Security	10-45
Hardware-Based Random Bit Generation (RBG)	10-46
High-Speed Encryption (HSE)	10-47
Image Steganography	10-48
Key Management	10-49
Key Recovery System (KRS) Failure Mode and Effects Analyses	10-50
Massively Concurrent Processing.....	10-51
Message Integrity and Non-Repudiation Authentication	10-52
Programmable, Embeddable COMSEC Technology	10-53
Pseudo-Random Number Generation	10-54
Quantum Computers	10-55
Quantum Encryption	10-56
Secret Sharing Schemes	10-57
Stream Ciphers	10-58
Zero-Knowledge Proofs (ZNPs)	10-59

DATA SHEET 10.4. CRYPTOLOGY

Developing Critical Technology Parameter	An example of basic research in mathematics, which could benefit existing cryptanalysis capabilities, is computational number theory research. In the next 15 years, number theory discoveries that could produce improved cryptanalytic techniques (e.g., more efficient solutions to the problem of factoring large integers) are possible.
Critical Materials	None identified.
Unique Test, Production, Inspection Equipment	None identified.
Unique Software	None identified.
Major Commercial Applications	Mathematics (cryptology) is the basis for the emerging strong dual-use cryptography. The INFOSEC industry supplies cryptographic applications to the financial services industry, telecommunications industry, legal and medical services, and the developers of a wide variety of e-commerce applications and personal privacy products.
Affordability	Not an issue.

BACKGROUND

Cryptology is a field of mathematics based on algorithms that perform calculations to encipher and decipher text, files, and data. Mathematics is a science that has been in the public domain for a long time, and cryptology is now widely studied in industry and academia. Number theory and discrete mathematics are important areas in this field. Continuing basic research in the cryptology branch of mathematics is needed to prove the strength of existing commercial cryptographic systems and to develop more robust protocols and more efficient cryptanalytic techniques and tools.

Increased commercial interest in cryptology has significantly influenced the search for potentially profitable new discoveries. Networks are driving commercial and government cryptology R&D programs toward stronger cryptography and protocols and improved cryptanalytic techniques. Improved cryptanalysis techniques could be the product of new discoveries in mathematics.

Although national governments are no longer the universal leaders in this field, governments universally classify cryptologic applications developed for military and government use. Some government-developed cryptology has been placed in the public domain [e.g., the data encryption algorithm in the Data Encryption Standard (DES) (FIPS Pub 46-2)]. The successor to DES, the Advanced Encryption Standard (AES), is now being developed and will also be placed in the public domain.

Efficient cryptanalysis systems are a key capability required for information dominance. The integration process will be the principal developmental effort required for military use of this technology.

Historically, governments have been the centers of cryptologic development. However, the civilian sector is now advancing the development, production, and marketing of cryptologic products. The business potential of networks is driving the commercial development of cryptography-enabled e-commerce applications.

DATA SHEET 10.4. DISTRIBUTED KEY GENERATION

Developing Critical Technology Parameter	Distributed key generation is the delegation of key generation to various entities (e.g., end users) in the public key infrastructure (PKI). Currently, many DoD systems use a central key generation facility.
Critical Materials	None identified.
Unique Test, Production, Inspection Equipment	None identified.
Unique Software	None identified.
Major Commercial Applications	A sound PKI is an important element of strong scaleable commercial cryptographic systems. The INFOSEC industry already supplies PKI systems, which are used by the financial service industry, the telecommunications industry, the legal profession, and medical delivery services. Many cryptography houses are developing a wide variety of distributed key generation PKI e-commerce applications.
Affordability	Not an issue.

BACKGROUND

Distributed key generation is fundamental to meeting the requirement for secure, scaleable cryptographic systems. The civilian sector uses various forms of distributed key generation in commercial systems. A proactive signature scheme might also perform distributed key generation, with each signing device generating its own key fragment pair internally.

A sound PKI is one of the most critical elements of a distributed key generation protocol. National and international standards bodies are working on PKI issues. The Federal Public Key Infrastructure (FPKI) Technical Working Group meets monthly and is moving rapidly to develop a standard for USG certificate management. A robust PKI that supports distributed key generation is a dual-use item that could be used by governments and military forces.

DATA SHEET 10.4. ELECTRONIC CASH (e-cash) TRANSFER SYSTEM

Developing Critical Technology Parameter	Interoperability of secure payment software among purchasers, merchants, and financial institutions is the difficult goal of standards organizations and most e-cash system developers. Trust is also an important characteristic of e-cash. All parties to the payment transaction must be assured that payment information will be protected from alteration and disclosure. It may take 5 or 10 years to establish complete e-cash transfer system interoperability and trust.
Critical Materials	None identified.
Unique Test, Production, Inspection Equipment	None identified.
Unique Software	None identified.
Major Commercial Applications	The major commercial applications for e-cash will be among the financial services and in e-commerce conducted over the Internet. Interest in e-cash is growing exponentially with the growth in e-commerce.
Affordability	Not an issue.

RATIONALE

The purpose of an e-cash payment system is to instruct a financial institution to make near-term payment to a merchant from a purchaser's account. E-cash transfer systems are an obvious target for those who might attempt to compromise U.S. economic security.

A significant form of e-cash, anonymous cash, raises issues that must be resolved by finding a balance between the privacy rights of the individual and integrity of the nation/state monetary systems. Forms of E-cash could make supply decentralization and savings possible.

DATA SHEET 10.4. ELLIPTIC CURVE SYSTEM SECURITY

Developing Critical Technology Parameter	Elliptic curves are gaining widespread acceptance. Several companies have already developed elliptic curve cryptographic systems. The USG may soon incorporate elliptic curves in USG Type 1 cryptographic systems. More basic research to discover proof of elliptic curve system security is needed. Additional research may firmly establish universal belief in their strength. It is critically important that their assumed strength be proven or established as soon as possible. In 5–15 years, the required proof could be discovered or their strength could be established.
Critical Materials	None identified.
Unique Test, Production, Inspection Equipment	None identified.
Unique Software	None identified.
Major Commercial Applications	The efficiencies of elliptic curve cryptosystems for authentication, data integrity, non-repudiation, and confidentiality are beneficial in military and civilian applications where computational power and IC space is limited, such as in IC Cards (“smart cards”), PC Cards [formerly Personal Computer Memory Card International Association (PCMCIA) cards], and portable and transportable wireless (RF) devices.
Affordability	Not an issue.

BACKGROUND

The security of elliptic curve systems—their main attraction—is based on the assumption that the analogue of a discrete logarithm problem in these curves is apparently much harder to solve than the discrete logarithm problem and the integer factorization problem that provide security in other public-key systems. Given current knowledge and processor power, elliptic curve systems are relatively strong. There are efficiencies in elliptic curve cryptosystems for applications in which computational power and IC space is limited.

With processor power doubling every two years and the constant threat of a cryptanalytic breakthrough, keys must be lengthened to maintain constant cryptosystem strengths. A relatively short (~ 160-bit) elliptic curve key is popularly believed to provide a strength that approximates the strength of discrete log and factorization public key systems using much longer (~ 1,024-bit) keys.

Several cryptographic suppliers will soon provide comparatively inexpensive tool kits for adding elliptic curve cryptographic functionality at standard cryptographic application programming interfaces (CAPIs). Elliptic curves may soon be incorporated in the digital signature standard (FIPS Pub 186). Elliptic Curve Cryptography (ECC), with its anticipated virtues, could become ubiquitous in small systems with limited bandwidth and processing power in civilian and military applications if full confidence in its comparative cryptographic strength is established.

DATA SHEET 10.4. HARDWARE-BASED RANDOM BIT GENERATION (RBG)

Developing Critical Technology Parameter	The security of many cryptographic systems depends on the generation of secret quantities or values in the form of random bits. In 10 to 20 years, it may be possible to generate improved random numbers with hardware or some combination of hardware and software, which are more nearly random and thereby increase the strength of cryptographic systems.
Critical Materials	None identified.
Unique Test, Production, Inspection Equipment	None identified.
Unique Software	None identified.
Major Commercial Applications	The major commercial application of hardware-based RBGs will be in cryptographic applications for use in e-commerce operations. More nearly perfect random bit strings will strengthen those cryptographic applications that depend on the randomness of bit streams for their strength.
Affordability	Not an issue.

BACKGROUND

Hardware-based RBGs can be used to exploit the randomness that occurs in some physical phenomena. Hardware generation is covered separately because it is different from pseudo-random number generation, which is often accomplished with software.

Hardware-based random number generators can be used to generate the seed for pseudo-random bit generators. This is important because cryptographic system keys must be generated efficiently. The most efficient way to generate the seed for pseudo-random bit generators is to produce strong keys. In many systems, this can be accomplished by using hardware rather than software. To meet the requirements of trusted systems, hardware-based RBGs in commercial products must pass the FIPS Pub 140-1 randomness tests.

Governments and industries are sponsoring random number and bit generation R&D. The goals of these basic and advanced research investigations are to find efficient, low-cost methods for generating random bits or capturing and converting natural noise for economical use in random bit generation. Many cryptographic system developers depend on various methods for the generation of pseudo-random bit streams.

DATA SHEET 10.4. HIGH-SPEED ENCRYPTION (HSE)

Developing Critical Technology Parameter	USG HSE R&D is for data rates in the 1 to 10 Gbits/sec range and is addressing a variety of challenges (e.g., how an originator authenticates in nanoseconds). The current front-end HSE work is concentrating on developing ATM technologies for even higher rates. Old approaches to data security and integrity and authentication and access control are not fast enough to cope with the new high-speed, broadband networks. HSE should be application ready in 10 years.
Critical Materials	None identified.
Unique Test, Production, Inspection Equipment	None identified.
Unique Software	None identified.
Major Commercial Applications	This is expected to become a dual-use technology because of the commercial requirement to increase the speed and security of communications. The financial service community and e-commerce interests are now demanding more bandwidth and more secure telecommunications for electronic funds transfer applications and various e-commerce applications.
Affordability	Not an issue.

BACKGROUND

HSE is a technology that could minimize the performance impact of secure communication services in high-speed networks [OC-12 (622 Mbit/sec) and above]. HSE is important because high-speed, real-time, dynamically reconfigurable, reliable packet switched networks are the predominant near-term way of implementing wide band.

DATA SHEET 10.4. IMAGE STEGANOGRAPHY

Developing Critical Technology Parameter	The human eye can detect only about 6 bits of information per pixel. Many image files have 8 bits. The lower two bits can be encoded covertly. A picture file could carry a 5–10-percent randomly embedded information set before it becomes statistically detectable. Binary executable files also can be encoded—but at a lower rate. In 5–10 years, even better image encryption and steganography techniques could be application ready.
Critical Materials	None identified.
Unique Test, Production, Inspection Equipment	None identified.
Unique Software	None identified.
Major Commercial Applications	Building on the current image steganography market, commercial uses for image steganography in the protection of intellectual property could be even wider. Copyrighted data could be watermarked with image steganography. Digital forms of works of art should be especially easy to watermark to provide proof of ownership or origin, as would any other electronic data image products sold in e-commerce over the Internet.
Affordability	Not an issue.

BACKGROUND

Steganography is that branch of cryptology that attempts to obscure the existence of data through the use of subliminal channels. Now, encrypted information can be randomly embedded in the quantization noise of image files and other data, without increasing the size of the host file.

Widely available steganographic programs can incorporate a 64-kilobyte message in a 1024 × 1024 grayscale picture without changing the graphical image noticeably. A new approach embeds data in images without making the changes to the image detectable. This technique could be used to send sensitive information over open communications lines. For additional strength, the information can be encrypted before embedding.

Image steganography could have many other applications (e.g., putting extra identifying features on documents, maps, and pictures). It could be used to guarantee the integrity of picture badges and identification cards.

Electronic data steganographic techniques are reasonably well understood and in the public domain. Comparatively inexpensive steganographic applications run on desk-top computers. Many good commercial applications, including shareware, are available in the Internet. Various forms of steganography have important intellectual property protection potential.

DATA SHEET 10.4. KEY MANAGEMENT

Developing Critical Technology Parameter	The <i>Infosecurity News Buyers Guide</i> for 1998 lists more than 27 data encryption key management products. Early versions of this technology are here now. However, it may be 10–15 years before systems are trusted for critical National Security functions and the Services are manned, trained, and equipped with trusted systems that support key management.
Critical Materials	None identified.
Unique Test, Production, Inspection Equipment	None identified.
Unique Software	None identified.
Major Commercial Applications	The civilian sector is advancing the development and production of commercial key management systems. Commercial applications are used by the financial service industry and in e-commerce. Certification authorities (CA) are not yet widely available to support the integrity of commercial public keys.
Affordability	Not an issue.

BACKGROUND

Key management is the most significant item in the critical path for the development and use of large cryptographic systems. The design of key management protocols is usually the pacing item in system development. Key management must certify the validity of keys that are put in service and promptly revoke those that are no longer valid.

The management of large numbers of keys introduces risks. A trusted third party (TTP) must certify the public key of each entity to bind the identity of an entity to its public key. If the TTP is compromised, all communications are insecure until new secure keys are established. Cryptography should be an integral part of all information systems, which is essentially transparent to end-users in the next 20 years. Trusted key management systems and protocols and trusted public key infrastructures and protocols are prerequisites.

**DATA SHEET 10.4. KEY RECOVERY SYSTEM (KRS) FAILURE
MODE AND EFFECTS ANALYSES**

Developing Critical Technology Parameter	Key escrow and recovery archiving systems are developing rapidly. However, the protocols for these systems do not have the proven integrity, predictability, and trust of the traditional protocols that involve only the sender and the recipient to guarantee the security of cryptographic keys. It may take 10 years before the technical strengths of these new protocols are accepted.
Critical Materials	None identified.
Unique Test, Production, Inspection Equipment	None identified.
Unique Software	None identified.
Major Commercial Applications	The commercial business requirement is for access to, or recovery of, stored encrypted data—not data in transit. There is no commercial business requirement for USG key escrow.
Affordability	Not an issue.

BACKGROUND

Key recovery is one aspect of the key management problem that stands out in importance. It is a broad term that applies to many different techniques that provide users with the ability to recover plain text from encrypted text, files, and data.

The whole area of key management must be investigated more intensively. In key escrow and recovery archiving systems, the risks associated with introducing a third party (escrow agent) into what has traditionally been a two-party (sender and recipient) model have not been established. There is almost no theoretical background on the effect of an escrow agent protocol on cryptographic system security, and there has been little practical experience with these systems on a large scale or with interoperation among systems built by different vendors. Any flaws that may exist in these third-party systems might be discovered early and inexpensively with more third-party protocol applied research emphasis now.

DATA SHEET 10.4. MASSIVELY CONCURRENT PROCESSING

Developing Critical Technology Parameter	A Whitney MCP/total object processing system (TOPS) machine could have an effective sustainable high-speed performance of > 125 Teraops (125 trillion operations per second) on all jobs, at very low life-cycle cost. The principal advantage of the Whitney machine is TOPS. With TOPS, all data, information and procedure specifications (programs) are, and must be, true objects capable of independent identification, specification, and accountability. An assembly line processor system (ALPS) is an assembly line, high-speed processing approach to the production of information products. This machine could be application ready in 15 years.
Critical Materials	None identified.
Unique Test, Production, Inspection Equipment	None identified.
Unique Software	None identified.
Major Commercial Applications	No specific commercial applications for MCP/TOPS Whitney computers have been developed because the computer is still in the concept development phase. However, the Whitney will compete for the same commercial customers who now use large main-frame computers and super computers. Their speed and optical bandwidth capability will make them ideal gateways for Internet service providers and data warehouse nodes.
Affordability	Not an issue.

BACKGROUND

This is a new information processing concept advocating a completely new computer architecture standard that could eventually replace the current von Neumann computer architecture with an all-hardware TOPS. The Whitney could be the eventual successor to the 100-Teraflop computer. The Whitney does not use a computer software "operating system." With the ALPS for Information (ALPS/I), all functions, usually provided by an operating system, are provided by hardware or hardware logic controlled by a read-only memory provided by the manufacturer. All information entered into the system must be in the form of true "objects." (An object is defined as a thing that can be identified and described independent of its environment and present or past use.) MCP/TOPS computers could be used for computation-intensive applications. With appropriate programming, MCP/TOPS computers could significantly shorten the time required for exhaustive key searches and the time required for computation-intensive operations, such as primality testing, key generation, and statistical tests to assess the strength of cryptographic algorithms. The MCP/TOPS will be a true dual-use item. The same basic processor should meet civilian commercial and military requirements. Fifteen years of development will probably be required for either commercial or military use. Additional development time will be required to develop the applications that will run on the Whitney.

DATA SHEET 10.4. MESSAGE INTEGRITY AND NON-REPUDIATION AUTHENTICATION

Developing Critical Technology Parameter	Protocols exist for message authentication, with message authentication code (MAC) and digital signature schemes to prove integrity and non-repudiation; however, these protocols have not been proven to the satisfaction of interested parties. To prove the security of message authentication and non-repudiation protocols, 5 or 10 more years of R&D may be required.
Critical Materials	None identified.
Unique Test, Production, Inspection Equipment	None identified.
Unique Software	None identified.
Major Commercial Applications	The major commercial applications will be those developed for e-commerce.
Affordability	Not an issue.

BACKGROUND

Message integrity and non-repudiation authentication convince a receiver of the identity of the message sender and message integrity. Non-repudiation provides the data sender proof of delivery and the data recipient assurance of the sender's identity, so that neither can later deny having processed the data.

More research is needed in the INFOSEC areas of message integrity and non-repudiation authentication. For example, scientific investigations should be made into the various impersonation attack and substitution attack methods against algorithms used in current and future authentication schemes. Methods should be developed for computing deception probabilities with which to specify the strength of authentication codes and their protocols.

DATA SHEET 10.4. PROGRAMMABLE, EMBEDDABLE COMSEC TECHNOLOGY

Developing Critical Technology Parameter	This technology provides INFOSEC functionality to a system on a modular basis. Support will be given to multiple algorithms simultaneously. This technology, because of its modularity, will reduce costs associated with accreditation. It could be application ready in 5–10 years.
Critical Materials	None identified.
Unique Test, Production, Inspection Equipment	None identified.
Unique Software	None identified.
Major Commercial Applications	Commercial applications were not identified; however, the programmable, embeddable COMSEC concept might make cryptography more affordable in commercial applications. Life-cycle costs could be reduced for some operating systems and applications if the programmable, embeddable cryptographic functionality could be ported from version to version. There could be significant savings in life-cycle costs.
Affordability	Not an issue.

BACKGROUND

Programmable, embeddable COMSEC technology allows the implementation of multiple, cryptographic services and algorithms simultaneously. It is an interoperability technique that places all critical security functions within a COMSEC module. This modular approach ensures that the approved security level will be maintained when host systems are modified or changed. As a result, hardware upgrades based on this technology are easier to implement, host interfaces can be changed and upgraded without impacting the INFOSEC requirements, and recertification efforts will be reduced significantly.

DATA SHEET 10.4. PSEUDO-RANDOM NUMBER GENERATION

Developing Critical Technology Parameter	There are several well-known pseudo-random bit generators (PRBGs) in use that are relatively fast and secure, such as those based on RSA™ and Secure Hash Algorithm (SHA-1) encryption functions. PRBGs that are based on the fundamental problem of factoring and the discrete logarithm problem may be proven to be secure, given some plausible computational assumptions. However, 10 or more years may be required before more efficient, provably secure, random number generators can be developed and proven to produce true random bit strings.
Critical Materials	None identified.
Unique Test, Production, Inspection Equipment	None identified.
Unique Software	None identified.
Major Commercial Applications	Improved random number generators will increase the security of commercial cryptographic systems used by the financial services industry and for e-commercial and individual privacy.
Affordability	Not an issue.

BACKGROUND

Deterministic (von Neumann) digital computers generate pseudo-random numbers that form a predictable, repeating sequence. The period of the repeating sequence can be so long that such pseudo-random numbers can be considered random for all practical purposes, except cryptography.

Pseudo-random number generation is a critical key generation function in most cryptographic applications. Secure keys for cryptographic systems must be generated efficiently with software in many systems.

Many forms of cryptography depend on random numbers employed to encrypt and decrypt voice and message traffic. Cryptography is extremely sensitive to the properties of random-number generators. Most state-of-the-art commercial cryptography and cryptographic tool kits have PRBGs included for key generation that will produce a sequence without any readily discernible pattern. However, FIPS Pub 140-1 specifies statistical random number generator tests for cryptographic modules that have to be incorporated in all common criteria security levels. Many pseudo-random bit generation methods are in the public domain, and pseudo-random bit generation technology is generally well understood.

A completely different approach to the generation of random numbers is covered in the hardware random number generator technology.

DATA SHEET 10.4. QUANTUM COMPUTERS

Developing Critical Technology Parameter	Scientists have shown that there is a possibility that “quantum parallelism” can be exploited to perform in a few seconds certain calculations that would take billions of years on the most powerful classical computers. It may be over 20 years before quantum computers are application ready.
Critical Materials	None identified.
Unique Test, Production, Inspection Equipment	None identified.
Unique Software	None identified.
Major Commercial Applications	There are no published reports of major civilian applications for quantum computers other than basic quantum research; however, there is wide international R&D interest, which suggests that there may be several potentially valuable commercial applications that are still proprietary, or in the case of governments, classified.
Affordability	Not an issue.

BACKGROUND

Scientists believe that ions trapped in an electric field and cooled to fractions of a degree above absolute zero could be coupled to produce quantum logic gates in a quantum computer. Quantum computers could make public key cryptography obsolete. A cryptographic quantum algorithm has been found for quickly factoring numbers so huge that they might take a time period the equivalent of the age of the universe (~ 12 billion years) to factor using current von Neumann processors and current state-of-the-art factoring algorithms. If quantum computers become widely available, public key cryptographic schemes based on the difficulty of factoring large numbers will be vulnerable.

Cryptanalysis is an important potential military application for quantum computers. The quantum computer could also be a valuable tool for basic and applied mathematics research and research in other complex fields e.g., weather modeling and forecasting. Quantum computers are not yet at the commercial technology stage, and years of development may be required before they are ready for military use. There is adequate access to this science and technology through the network of interested international scientists and multinational corporations performing quantum computer research.

DATA SHEET 10.4. QUANTUM ENCRYPTION

Developing Critical Technology Parameter	Laboratory researchers are experimenting with quantum encryption, which theoretically could provide an unbreakable system for protecting messages sent over fiber-optic cables. In the next 15 years, discoveries that could produce transmission capabilities over long distances and improved quantum encryption techniques may be possible. This technology could be application ready in 20 years.
Critical Materials	None identified.
Unique Test, Production, Inspection Equipment	None identified.
Unique Software	None identified.
Major Commercial Applications	No immediate commercial applications for quantum encryption were identified.
Affordability	Not an issue.

BACKGROUND

Quantum encryption takes advantage of the Heisenberg uncertainty principle, which holds that the accurate measurement of an observable quantity necessarily produces uncertainties in the knowledge of the values of other observables. If encrypted information were inserted into the quantum properties of individual photons in an optical path, cryptanalysts would be unable to attack the messages without altering them. They could determine a photon's location, or they could determine its energy; however, they could not determine both properties without destroying the message, because if they stop the photon along its optical path, they alter its quantum characteristics.

Extensive development of this technology will be required before it will be ready for military use. Under laboratory conditions, this technique inserts information into the quantum properties of individual photons. Each photon carries a single bit of data. By placing the encrypted information in the quantum states of photons, scientists have been able to provide interception-proof encryption in the laboratory. At present, this is a laboratory artifact and has not progressed to the point at which it could be commercialized.

DATA SHEET 10.4. SECRET SHARING SCHEMES

Developing Critical Technology Parameter	Secret sharing schemes are at the heart of some key recovery systems in which several participants in the access structure may hold portions of the key. The key must be shared in such a way that only authorized subsets can determine the key. Various forms of this technology are application ready now; however, mathematically provable schemes may be 5–10 years away.
Critical Materials	None identified.
Unique Test, Production, Inspection Equipment	None identified.
Unique Software	None identified.
Major Commercial Applications	Secret sharing schemes are used by the financial services industry to protect master keys. CA use secret sharing schemes to protect the root private key. Many commercial enterprises use secret sharing schemes for key recovery in case emergency access is required.
Affordability	Not an issue.

BACKGROUND

Cryptographic secret sharing schemes are various methods of sharing a key among a limited set of participants. The USG key escrow scheme (FIPS Pub 185) is a form of secret sharing in which the law enforcement access field (LEAF) portion of a cryptographic key is divided between two agencies and then re-divided within each agency, in effect providing four-person control. Most commercial key recovery schemes also use some form of secret sharing.

Although some secret sharing schemes in the public domain are fairly mature, others will require further development. Integration of the commercial secret sharing features and protocols with other functionality in military applications is required.

DATA SHEET 10.4. STREAM CIPHERS

Developing Critical Technology Parameter	There is a large body of theoretical knowledge on stream ciphers. Various design principles for stream ciphers have been proposed and extensively analyzed and could be significantly advanced and be application ready in 10 years.
Critical Materials	None identified.
Unique Test, Production, Inspection Equipment	None identified.
Unique Software	None identified.
Major Commercial Applications	The same characteristics that make stream ciphers of value in secure military systems make them of value in protecting civilian network traffic. Eventually, all network traffic will be protected by link encryption, end-to-end cryptography, or both. Business, industry, and personal network applications will also be required to perform in situations where transmission errors are probable.
Affordability	Not an issue.

BACKGROUND

Stream ciphers operate on the plaintext a single character at a time. The security of the system depends solely on the keystream generator, which outputs a stream of bits that are combined with plaintext bits to produce a stream of ciphertext bits. The keystream changes with every character. Stream ciphers are generally faster than block ciphers and are easier to implement in hardware. They may be more affordable for certain telecommunications applications in which buffering is limited or characters must be individually processed as they are received. Error propagation, which depends (among other things) on the length of the internal registers used in the keystream generator, can be limited.

Stream ciphers are also advantageous in situations where transmission errors are highly probable. There is a comparatively small body of open source stream cipher literature. In combat situations where transmission errors are probable, stream ciphers will introduce little error propagation. They are used for applications in which the data must be processed one symbol at a time and in equipment that has no memory or in which data buffering is limited.

DATA SHEET 10.4. ZERO-KNOWLEDGE PROOFS (ZNPs)

Developing Critical Technology Parameter	A variety of ZNP protocols specifically designed to achieve identification could be application ready and have practical use in 10 to 15 years.
Critical Materials	None identified.
Unique Test, Production, Inspection Equipment	None identified.
Unique Software	None identified.
Major Commercial Applications	The ZNP characteristic of anonymity is an important part of some concepts for e-commerce transactions. Proof of certain generic authority or credit "credentials" might be provided for e-commerce by using ZNP systems.
Affordability	Not an issue.

BACKGROUND

ZNPs are methods for proving knowledge of a secret without revealing any knowledge of the secret (e.g., proving knowledge of a key without revealing anything about the key). ZNP protocols provide trusted authentication mechanisms and anonymity. For example, one could prove U.S. citizenship or majority without providing any other specific information such as name, address, or exact age.

SECTION 10.5—INFORMATION MANAGEMENT AND CONTROL

Highlights

- Information Management and Control (IM&C) FA capabilities are fundamental to normal day-to-day and stressed-mode complex system operations.
- As ISs grow and add more components, more functions, and more users, IS IM&C becomes more difficult and complex—yet increasingly important.
- Adequate IM&C capabilities are necessary to convert civil telecommunications or other complex IS systems to military use.

OVERVIEW

The IM&C FA is defined as capabilities to plan, organize, design, optimize, engineer, implement, operate, monitor, provision, maintain, synchronize, supervise, manage, control, and administer entities, systems, elements, processes, organizations, and events. Demonstrating the breadth of IM&C functionality, each capability item implies additional or subsidiary capabilities. For example, in telecommunications systems, the ability to “monitor” normally implies comprehensive performance assessment facilities to detect, isolate, report, and record network faults; to measure offered and refused (busy condition) traffic; and to measure call completion items, call duration, and numerous other parameters critical to efficient operations.

IM&C refers to both the capability to manage and control information, information operations (IOs), and information systems (ISs), as well as ISs configured to manage and control entities, systems, devices, processes, organizations, and events whose primary purpose and application are other than information operations or systems.

Historically, most advanced IM&C technology and standards developments have been related to ISs, in general, and telecommunication systems, in particular. Fortunately, because the variety of telecommunications services, operations, configurations, and devices is so great, the bulk of such work produces “generalized” paradigms, architectures, communications protocols, and managed-object naming and attribute description conventions that can be applied to almost any IM&C requirement.

The strategy and rationale underlying modern IM&C design is best described by the conditions and impetus that led to the development of today’s advanced technologies. Until the mid-to-late 1970s, telecommunications networks supported limited sets of services derived from a relatively small set of basic technologies and used equipment from only a few vendors. As we begin a new century, divestiture, deregulation, privatization (overseas), and rapid technological expansion have resulted in significant growth in the number of private and public telecommunications networks. These networks support a myriad of services derived from wide varieties of network elements and use equipment supplied by hundreds of manufacturers.

To cope with the added functional complexity, while reducing manpower requirements, network operators are placing more processors in voice communications networks (VCNs). Analogously, the trend away from centralized mainframe designs and the immense popularity and exponential growth of the Internet have spawned a large number of data communications networks (DCNs), which are now needed to connect distributed processors in client/server configurations. Networks are now more complex and software driven than ever.

Not surprisingly, as networks proliferate and add more components, more functions, more users, and more automation, network management (NM) becomes more difficult and complex yet increasingly more important. For example, in the United States, divestiture has meant that many end-to-end connections require services and/or facilities from two local exchange carriers (LECs), one or more interexchange carriers (IXCs) or backbone networks, and often two local area networks (LANs) comprising customer premises equipment (CPE) from a variety of manufacturers. End-to-end service management, therefore, requires not only the IM&C of each separately owned

LEC/IXC/CPE domain, but an “integrated management and control” capability spanning all domains connected to and “interoperable” with each “managing entity.” In overseas markets, similar situations exist among interconnected pan-European national networks and in countries where privatization has spawned a variety of alternative service providers.

The fast-growing cellular telephone industry, particularly for roaming applications where one carrier’s subscribers must be recognized and served by other carriers’ networks, adds new dimensions to telecommunications management. The emerging mobile communications industry has also highlighted the urgent need to couple or integrate “technical” and “business” management and control. In early cellular systems, customer service representatives, with access only to account information, had no way of confirming or dealing with customer-reported “dropped-calls” or other outages. Modern designs anticipate customer-service-representative needs for highly integrated, user-friendly, graphical user interface (GUI)-based access to business accounting, marketing, and technical IM&C data and processing capabilities. As competition and technology reduce basic telecommunications services to commodity status, true market discriminators among alternative carrier and service provider offerings must be derived from what can best be described as telecommunications “business management.”

From a technical and implementation viewpoint, this multi-functional, multi-network, multi-domain, heterogeneous vendor equipment environment poses enormous end-to-end IM&C challenges and creates a large demand for advanced, standards-based NM technologies. To meet this demand, competing companies quickly introduced numerous proprietary, vendor-specific NM products to the market. At one point, a large computer company assigned 1,000 people to NM. In another large company, NM was the third largest development project in its history. Over 120 vendors offering NM products are now enrolled in another’s “partnership” program—illustrating the high level of industry interest.

In the mid 1980s, the worldwide standards-setting organizations recognized NM’s essential role in complex networks and the lack of compatibility among early NM products, and they embarked on the development of architectures and frameworks for interoperable telecommunications NM systems. In the VCN arena, the European Telecommunications Network Operators (ETNO), the European Telecommunications Standards Institute (ETSI), the European Conference of Postal and Telecommunications Administration (CETP), and the European Institute for Research and Strategic Studies in Telecommunications (EURESCOM) produced architectures and strategic plans incorporating standards-based, pan-European integrated NM systems. In particular, the ITU Telecommunications Sector Study Group IV and the ETSI NA4 Technical Subcommittee are completing a set of standards (the M.3010 recommendations) entitled *Principles for a Telecommunications Management Network (TMN)*.

In the DCN arena, the three principal standards activities are as follows:

- The International Standards Organization (ISO) has been working on Open Systems Interconnection (OSI) NM standards. OSI standards include the Common Management Information Protocol (CMIP), the Common Management Information Service Element (CMISE), and several subsidiary standards.
- The Internet Activities Board (IAB) has spearheaded the development of two NM standards: the Simple Network Management Protocol (SNMP) (versions v.1 and v.2) and the Common Management Information Services Over TCP/IP (CMOT).
- The Institute of Electrical and Electronic Engineers (IEEE) has assumed the lead role in defining management standards for LANs and metropolitan area networks (MANs). IEEE has also produced a draft standard entitled *LAN/MAN Management*. When CMIP is used in conjunction with IEEE standards, such use is often referred to as CMIP Over LLC (CMOL).⁶

Important aspects of these standards and the impact on NM and control technologies are summarized below. Perhaps more than in any other IS FA, IM&C technology value and criticality are determined by the degree to which “open-system” operations are available and supportable by practical and affordable products. For this reason, as a basis and rationale for including specific IM&C technologies, the remainder of this Overview focuses on emerging,

⁶ LLC stands for Logical Link Control.

standards-based, interoperable IM&C architectures, functional designs, protocols, device naming, and attribute specification conventions.

The ISO's Management Framework Standards, ITU-TS X.700, recommendations and the Internet Activities Board's requests for comments (RFCs) characterize management systems as consisting of the following components:

- A Structure of Management Information (SMI)
- A Management Information Base (MIB)
- A management protocol such as CMIP or SNMP.⁷

ISO/Internet management frameworks are based on the Agent Process/Manager Process paradigm, depicted conceptually in Fig. 10.5-1. A management process is defined as an application process responsible for management activities. Resources supervised and controlled by NM are called managed objects. An agent process performs management functions on managed objects. Agents often reside in managed objects, reporting the object status to a manager and responding to manager queries and other controlling commands.

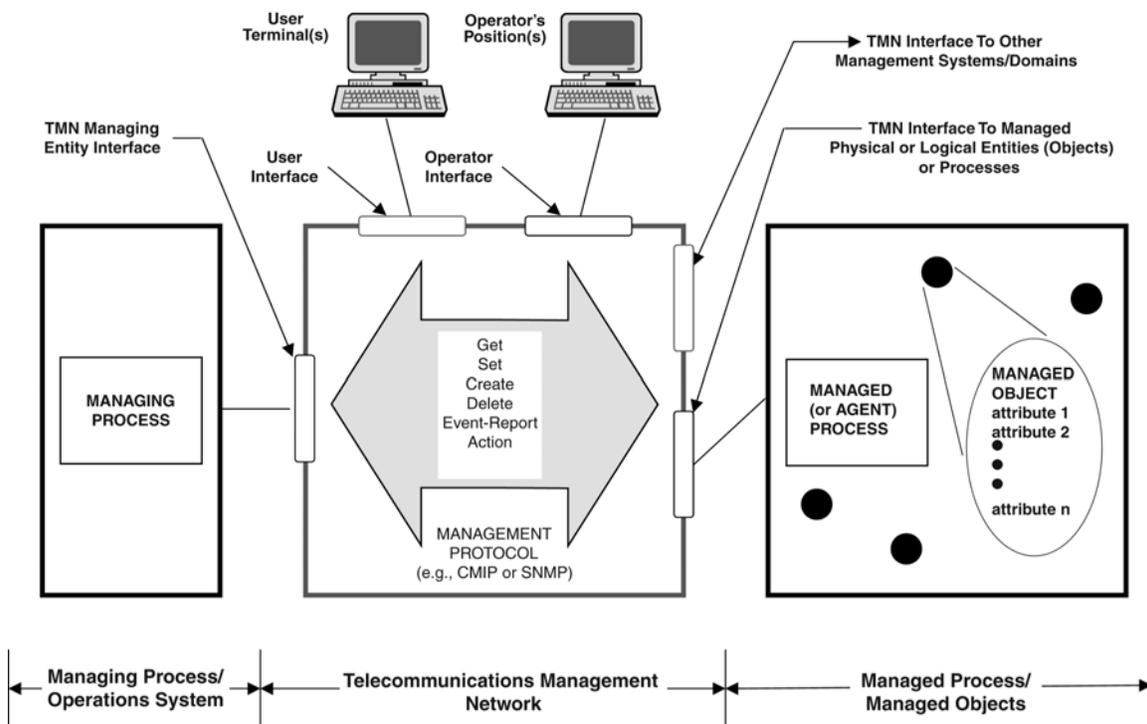


Figure 10.5-1. Agent Process/Manager Process Paradigm

Managers possess initial and updated global information on whatever physical or logical entity (object) the management system is designed to administer. These entities might be business applications, telecommunications services, physical networks, network elements, or network protocol layers. Managers—implemented in single consoles or within ensembles of distributed consoles—include GUIs, databases, and facilities to communicate with the objects they manage. The consoles enable human managers to access and invoke a variety of software management applications (configuration control, performance monitoring, fault isolation, diagnostics, and so forth). GUIs display *inter-alia* topologies of managed objects. Typically, operators can retrieve related status and MIB information stored in database repositories by simply “clicking” on objects depicted on a GUI display.

⁷ Protocols are strict procedures (implemented in transmitting and receiving devices) for the initiation, maintenance, and termination of data communications. Protocols define the syntax (arrangements, formats, and patterns of bits and bytes) and the semantics (system control, information context or meaning of patterns of bits or bytes) of exchanged data and numerous other characteristics (e.g., data rates, timing, and so forth).

MIBs define information about managed objects. Within MIBs, managed objects are described in terms of object attributes and characteristics, operations performed by or on object, notifications or reports objects can make, and an object's behavior or response to operations performed on it. The SMI identifies information structures describing managed object attributes, operations associated with attributes (e.g., "get," "set," "add," "remove"), and operations relating to the managed objects themselves (e.g., "read," "delete," "action").

With hundreds of network-managed product vendors and even larger numbers of managed network elements, the absence of object naming, attribute, and communications protocols standards would render "open system" IM&C impossible. In Fig. 10.5-1, the telecommunications management network (TMN) provides communications among managing and managed entities, is always logically distinct from "managed networks," and, where possible, is implemented on separate, highly redundant and reliable facilities. In addition to the managing and managed entity interfaces, the TMN also provides interfaces to "workstation functions" (i.e., both operator and user of customer terminals) and an interface to TMNs in other management domains.

Just as fourth-generation languages are shifting significant software development capabilities directly to end users, remotely programmable managed objects and advanced IM&C technology are shifting the ability to "design and build" software-defined complex systems and networks directly into the hand of network managers. For example, "virtual private networks" (VPNs) or software defined networks (SDNs) provide services that are virtually indistinguishable from yesterday's custom-designed "private networks" but are carried on public networks at rates significantly lower than dedicated facilities-based service costs. Moreover, most features and network design and configuration options can be selected from operator management consoles, with some control available directly from customer terminals. Thus, the role of network managers now includes negotiations of service-level agreements with users and the network design tasks necessary to fulfill those agreements—tasks previously allocated to third-party network designers.

This new role and the increased burden of performance management, fault isolation, current configuration, and trouble-history tracking in today's more complex and software-driven networks place a premium on a more capable, credible, and usually larger NM staffs. Offsetting this demand for human resources are intelligent alarm correlation; applications of rules and case-based reasoning for performance monitoring; fault isolation and trouble-ticket generation; use of time- and object-oriented software and databases; and natural language processing. These technologies are now being embedded in advanced IM&C designs. Of particular importance are the modular and scalable expert system approaches that accommodate a range of capabilities and the exponential growth of data, cellular, personal communications, and other popular services.

LIST OF TECHNOLOGY DATA SHEETS
10.5. INFORMATION MANAGEMENT AND CONTROL

Network Management 10-66

The following developing technologies have been identified, but data sheets are not available at this time:

Anomaly Prediction, Detection, and Diagnosis

Automated Self-Protection

Distributed Process Management (Systems Engineering)

Meta Management

Meta-Data Network Manager

Process and Data Mirroring Techniques

DATA SHEET 10.5. NETWORK MANAGEMENT

Developing Critical Technology Parameter	Bandwidth and transmission speed.
Critical Materials	None identified.
Unique Test, Production, Inspection Equipment	None identified.
Unique Software	Server operating systems, network fault detection, network performance monitoring, network security services, storage back-up and mirroring, network mapping, and network routing optimization.
Major Commercial Applications	Internet usage by general public.
Affordability	Cost will be less than current solutions.

BACKGROUND

Processing of applications and storage of data and information will become available to users who do not have a powerful computer as an access device. Many of these I/O devices will be very small, with just a chip for any kind of computing power. Some current examples are mobile phones or credit-card types of devices. In many cases, even users with a PC will not necessarily use the PC for anything more than a workstation.

A network of servers would do processing. The servers would contain all the software applications, the users' databases, and any parameters needed to specify user preferences in presentation. The servers would also have password information or any other personal identification to verify the user's identity. Currently on the Internet, several commercial sites obtain information on the user and user preferences. These sites contain all the application software and the database of common information and the database on the user preferences. A primitive example of this type of site would be Amazon.com, which recognizes a user accessing the site and charges items and makes suggestions based upon previous data on customer usage and preferences.

With processing and data storage becoming the function of the server, users will expect the server to perform all functions of any responsible computer services provider: data protection, privacy, security, availability, performance assurance, fault detection, software maintenance, tamperproofing, and reliability. Thus, the server will become a system as comprehensive and complex as just about any mainframe computer or transaction server known today. Users would be burdened by nothing more than a mobile device that possibly accepts nothing more than voice input and provides small-screen output or even just audio output.

SECTION 10.6—INFORMATION SYSTEMS FACILITIES

Highlights

- Older military or commercial high-technology, highly survivable transportable/mobile IS facility capabilities are readily available to proliferants.
- Advances in processing power, coupled with dramatic reductions in space, weight, and power consumption, allow IS capabilities to be packaged in much smaller volumes.
- In many cases, the total cost per transportable IS facility may be an order of magnitude less than the cost of a single precision-guided conventional weapon.

OVERVIEW

The Information System Facilities Functional Area is defined as capabilities to house, protect, energize, and transport IS infrastructures, providing them with appropriate operating, human habitation and life-support conditions under benign, naturally-occurring hazardous, or man-made conventional, chemical, biological, or nuclear warfare threat-driven environments. In this context the word “facilities” is used differently than when it is used, for example, to denote transmission media and other hardware in telecommunications systems.

Information System facilities encompass any or all of the following capabilities: exterior physical shelters or interior room partitioning; IS equipment and other supporting structures; conventional and/or co-generated prime power equipment; power conditioning; environmental heating, ventilation and air-conditioning (HVAC); chemical, biological and particulate filtration and other air-quality mechanisms; integrated, intelligent-building systems; electromagnetic pulse (EMP) protection; TEMPEST and radiation shielding; fire and other natural hazard safety measures; intentional physical and psychophysiological attack resistance and protection (including counter-terrorism capabilities and designs); trespass, theft and perimeter defense and intrusion detection systems; physical and psychophysiological efficiency and work enhancement means; and, human habitation and life-support accommodations. Civil and commercial IS shelters often do not include sleeping quarters or other personal accommodations, but instead support only work-related activities. Clearly, not all capabilities are required in every instance of military, civil, commercial or individualized operations.

Physical shelters may be fixed, or transportable in ground mobile, airborne or shipborne configurations. They may support manned command, control and intelligence centers, manned information processing or communications centers, or unattended IS resources. Unmanned facilities are often designed to resist or prevent intentional physical or functional damage, tampering or theft, and to exhibit automated maintenance, repair, disaster detection and recovery in reliable and secure manners. All facilities may be required to support covert offensive and defensive operations. To the extent that the cost of information facilities and contents can be reduced to acceptable levels, in some scenarios self-destruction by remote detonation or other means may be viable defensive strategies for unmanned facilities and in other circumstances when human safety concerns are assured. Figure 10.6-1 is a taxonomy of major IS facilities capabilities.

From a U.S. perspective, preparation for global nuclear warfare, beginning with the World-Wide Military Command and Control System (WWMCCS) program in the 1970s, led to the investment of billions of dollars in mobile, military, command and surveillance center technology. The airborne command center, the Airborne Warning and Command System (AWACs), and the Ground Mobile Command Center (GMCC) are illustrative developments. For tactical scenarios, the Tri-Services—Tactical Communications (TRI-TAC) program developed a wide variety of mobile/transportable voice and data switching, communications satellite and terrestrial terminals, and various IS processing center products to support moving-battlefield theater operations. In Europe, the Deutsche-Bundespost placed cable hocks within civilian telecommunications networks, permitting mobile switching and multiplexing gear

to be connected with surviving transmission media to restore service interrupted by intentional or collateral wartime damage.

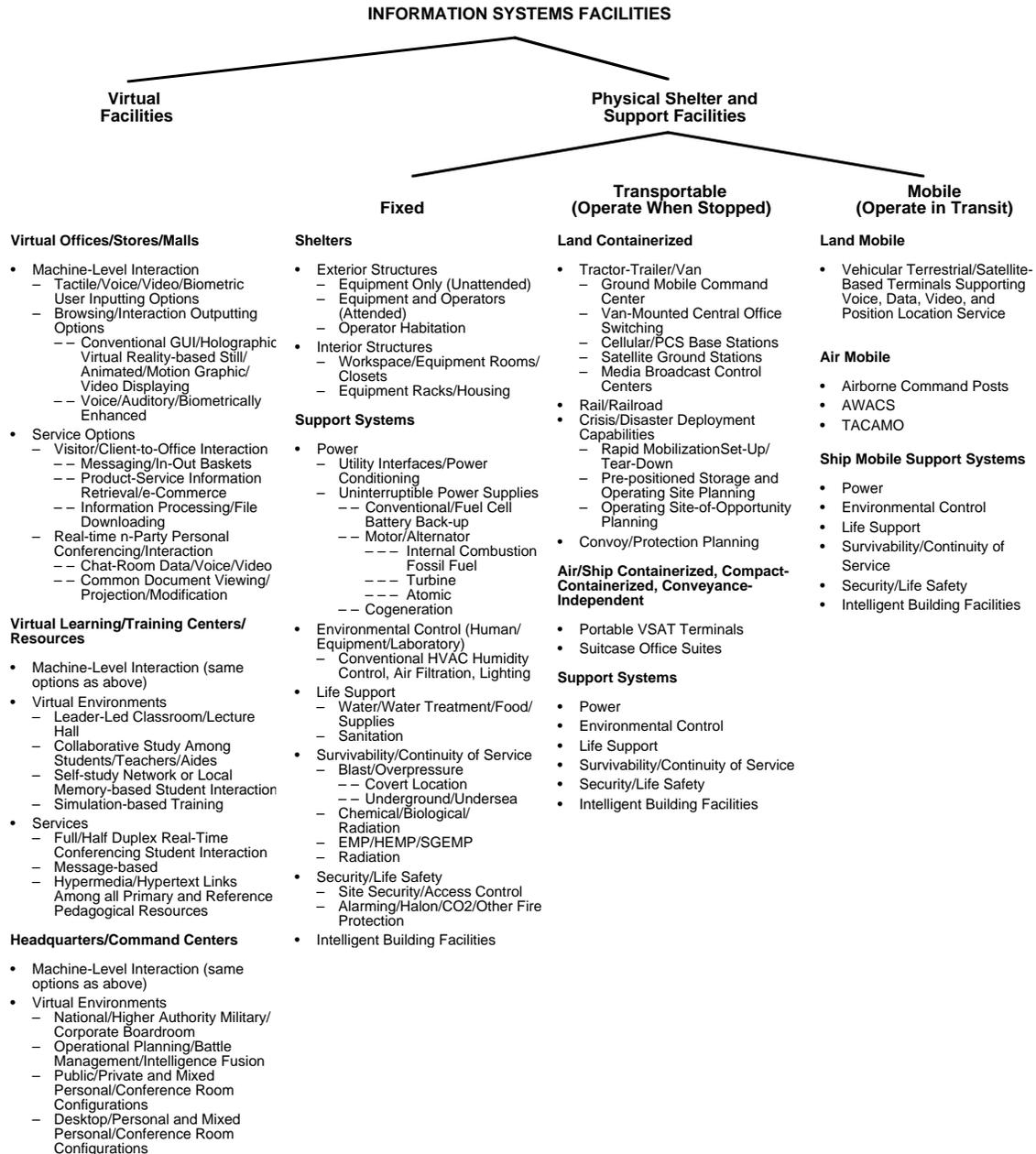


Figure 10.6-1. IS Facilities Capabilities Taxonomy

Because of these advances, the trend toward transportable IS facilities accelerated in the 1990s. Today, satellite terminals able to operate in military or civilian bands are encased in suitcases. COTS “office in suitcase” products incorporate multimedia telecommunications, position location devices, and rich varieties of distributed computing environment data processing functions. Worldwide, many commercial telecommunications carriers inventory central office, tandem, and dual-function switches; cellular/Personal Communications System (PCS) base stations; digital loop carriers (DLCs); and other capabilities in transportable/mobile configurations. Alternately, with broadband, fiber-optic transmission, traffic can be affordably back-hauled great distances to restore damaged or otherwise failed

switching, multiplexing, or other facilities (equipment) remotely. Because so many commercial enterprises now depend upon continuous telecommunications and data processing operations and because downtimes of even 15 minutes can have catastrophic revenue and profit consequences, many businesses have elaborate internal or third-party, contract-based, disaster recovery IS capabilities.

Figure 10.6-1 lists an emerging and increasingly important class of IS facilities best described as “virtual facilities.” All “Virtual Facility” users must reside in some “physical facility.” This means that no matter how advantageous they may be, virtual facilities can never totally supplant physical counterparts.

Virtual facilities are a form of virtual reality (VR), which is a computer-generated environment with which and within which people can interact. VR encompasses a range of interactive computer environments, from text-oriented on-line forums and multiplayer games to complex simulations that combine audio, video, animation, or three-dimensional (3-D) graphics and scent. Some of the more realistic effects are achieved using a helmet-like apparatus [e.g., head mounted displays (HMDs) or binocular omni-oriented monitor (BOOM) displays], often with tiny computer screens, one in front of each eye and each giving a slightly different view so as to mimic stereoscopic vision. Sensors attached to the participant (e.g., gloves, bodysuit, footwear) pass on the person’s movements to the computer, which changes the graphics accordingly to give the participant the feeling of movement through the scene. Computer-generated physical feedback adds a “feel” to the visual illusion, and computer-controlled sounds and odors reinforce the virtual environment. Other VR systems, such as flight simulators, use larger displays and enclosed environments [e.g., Cave Automatic Virtual Environment (CAVE) four-to-six-wall graphic projection mechanisms] to create an illusion of virtual presence. VR is becoming prevalent in electronic games, in amusement-park attractions, and for simulating design, construction, and other industrial development projects.

Less-complicated systems for personal computers manipulate images of 3-D space on a computer screen. Actual, experimental, and envisioned uses encompass electronic mail-based commerce (e-commerce, as manifested in virtual offices, stores, and malls); education and training (to include a variety of virtual classroom, distance learning, and telepresence capabilities); virtual headquarter and command centers; so-called “chat rooms”; industrial design; surgical training; art; and others. Figure 10.6-1 lists examples of currently popular virtual facilities.

BACKGROUND

IS facilities intended for human occupancy often require security mechanisms to reliably identify people authorized to enter facilities and to deny access to unauthorized people. In environments where people are cooperative, recognition and authorization to enter can be accomplished by a combination of technologies selected on the basis of perceived threats and the consequences of unauthorized entry. Since physical security measures are a continuing overhead cost, techniques applied must be judiciously selected.

Techniques for identifying individuals encompass finger, thumb, or palm-print analysis; multispectral image analysis of iris or retinal characteristics unique to an individual’s eye; handwriting; fast Fourier transform analysis of human voice harmonic content; absorption spectroscopy; bio-photonic fluorescent properties of an individual; physical body characteristics; or by all or any combination of these. Validating identity through combinations of these physical and physiological properties virtually eliminates unauthorized entry since it is nearly impossible to counteract living biological characteristics. Such security access measures are applicable to both attended and unattended facilities.

In some designs, attempted unauthorized entries automatically alert security teams or assigned tactical reaction forces; record the details of attempted entries; and, log events at remote sites so that the sequence of events will be preserved if the attempted entry proves successful and local records are destroyed.

Typically facility protection involves the continuous monitoring of indoor and outdoor environments. Sensors for environmental variables report ambient air and hardware temperatures, humidity, inundation, vibration, fire, barometric overpressure, selected gas partial pressure ratios, chemical agents, people or object movement, alternating current (AC) and direct current (DC) bus parameters, coolant failure, and RF activity. Automation and robotics permits monitoring of facilities too dangerous for human presence or monitoring multiple areas when insufficient numbers of people are available to cover all locations.

Facility access and egress control can require communications among people not sharing a common spoken language. Technologies are available that determine a speaker's native language and support dual-translation. Translation modes can be optional: that is audio voice, video narrative displays, print, or any combination.

Similar progress is evident in the "virtual classroom or university" domain. Here, at least initially, the most striking successes occur when a technological or an arts and sciences subject matter is so new that no single college or university has sufficient instructor expertise or other resources to offer comprehensive curricula. The emerging biocomputing field is noteworthy because in response to those needs, significant research, distance learning, and database sharing are already taking place via the Internet.

International standards and advanced objected-oriented software that enable "open-systems" interoperability among competing vendor services and products are facilitating—and indeed fueling—rapid growth in e-commerce, with its virtual stores and malls; teleconferencing-based virtual conference rooms and headquarters; and leader-led, self-study and collaborative forms of educational VR.

Key high-tech standards include the ITU-TSS G and H suites that define encoding, encryption, inter-codec (encoder-decoder) signaling, video, voice, imagery and graphics link multiplexing, link initiation/disconnect, and so forth. Also important are the Joint Photographic Experts Group (JPEG) and the Moving Pictures Expert Group (MPEG) standards for compression of still-photograph and moving-picture digital signals.

At the heart of all virtual facility designs is the ability to support multiple users simultaneously, with some level of interactive features. In virtual merchandize marts, for example, users (customers) can search for and, at a minimum, browse through "text-based" product information. More elaborate accommodations allow users to navigate through and examine a spatially oriented environment. This may be a graphical representation of an actual physical store and often allows users to "pick-up" objects and view them from any angle.

Still-more-elaborate designs allow users to interact in real time with each other and with processor-based virtual facility features, such as those mentioned previously. Chat rooms are a low-end, text-based example. However, many virtual classroom, headquarters/command center, and other network-based decision support arrangements offer sophisticated voice, video, graphics, and imagery operational capabilities that make electronic collaboration equal to or, in some circumstances, preferable to what can be accomplished in physical face-to-face meeting places.

Predecessors of today's technology include early (1979) multi-user interactive role-playing games on the Internet, most of which employ Multiple User Dimensions (MUDs). MUDs are synchronous (real-time), text-based multi-user VR environments that allow users to interact with the environment and with other users. MUD Object Oriented (MOO) is most popular in education VR since it employs a highly sophisticated, built-in programming language. The development of more flexible and powerful virtual facility technologies will be important in future military training.

No matter how potent virtual facilities may become, they can only be accessed by human users via some sort of physical facility. Such physical facilities fall into two broad categories:

- There are large, multi-person, private or public teleconferencing facilities usually equipped with full complements of large-screen displays, automated and/or manually directed audio and video equipment, and leader-led and individual participant-controlled text and graphic information I/O and presentation devices.
- At the other end of the spectrum are PC-based terminals that enable individuals to observe passively conferences, decision-making, or learning sessions or to interact actively with other individuals and/or machine-based intelligent processes in those sessions.

In either "large complex" or "personal" physical facility cases, users may be furnished with conventional "PC-like" keyboard and audio and visual I/O devices. For more complete immersion in and with virtual-facility cyberspace, users may be equipped with more exotic HMD, Binocular Omnidirectional-Oriented Monitor (BOOM), Computer-Aided Engineering (CAE)-type displays, and other apparatus.

LIST OF TECHNOLOGY DATA SHEETS
10.6 INFORMATION SYSTEMS FACILITIES

Finger, Thumb, and Palm-Print Identification 10-72
Wearable Computing Systems (WCSs) 10-74

The following developing technologies have been identified, but data sheets are not available at this time:

- Absorption Spectroscopy
- Automated Self-Protection
- Automated Video Identification
- Correlation Techniques for Validation of Identification
- Environmental Monitoring
- Lasers (for Transmission Over Fiber Optics)
- Personal Identification, Cooperative
- Personnel Identification (Specific and Generic), Uncooperative
- Robotics (Free-Roaming)
- Selectable Communications Mode [Audio, Video, Print, Virtual Reality (VR)]

DATA SHEET 10.6. FINGER, THUMB, AND PALM-PRINT IDENTIFICATION

Developing Critical Technology Parameter	Processing speed.
Critical Materials	None identified.
Unique Test, Production, Inspection Equipment	None identified.
Unique Software	None identified.
Major Commercial Applications	Financial institutions.
Affordability	Other biometric identifiers may become less costly for the reliability offered.

BACKGROUND

Finger, thumb, and palm-print identification technologies are closely related to the technologies that appear in the Information Systems Security subsection (9.4), almost all of which require positive identification of individuals participating in USG and civilian critical IP functions—with a “true” identity validation probability approaching 1.0. For brevity, “fingerprint identification” is used as a collective term in this technology item. By definition, fingerprint identification systems include both overt and surreptitious finger, thumb, and palm-print data capture, correlation, analysis, display, storage, and retrieval elements.

In ancient China, rulers sealed important documents with thumbprints. Now, fingerprint imaging is the most commonly used method of biometric recognition. Other biometric technologies are also based on identifiable traits, which can include hand contours, retinal patterns, voice patterns, keystroke rhythms, and handwriting acoustic emission. There are still other emerging biometric technologies in the research stage. Some, such as knuckle creases, hand veins, acoustic head resonances, and even body odors, seem a little bizarre. Fingerprint identification technology is relatively mature, reasonably accurate, and more acceptable legally than other biometric technologies. However, fingerprint identification is far from absolute. Because the current fingerprint identification system hardware, software, and protocol elements introduce significant uncertainties, priority R&D by the USG and industry is required.

Experts generally agree that one in every 50 people have fingerprints that today’s technology cannot handle. Even at the Federal Bureau of Investigation (FBI), which handles between 30,000 and 50,000 fingerprint cards every day, one of every ten prints checked in 1998 was not clear enough to provide positive identification. Because of variations in sensor contact pressure and the angle and location of the fingerprint area in relation to the sensor, no two consecutive captures of the same fingerprint data are identical. Fingerprint data capture software robustness is not yet sophisticated enough to compensate for fingerprint positioning variations. The technical specifications, standards, and test protocols required for unbiased fingerprint identification product evaluations have not yet been developed. Highly adaptable and easily integrated fingerprint identification systems that have a universal probability of positive identification approaching 1.0, with very low false acceptance ratios (FAR), may be 10–15 years away, depending on the priority given this technology by the USG and industry.

Positive identification and subsequent verification of a person open up new ways of providing vertical services to more people. Positive identification is not a blessing in the view of a significant minority. There is a “Fight the Fingerprint” web site, which argues against fingerprint identification, making the proclamation “We stand firmly opposed to all government-sanctioned biometrics and social security number identification schemes!” Civil libertarians warn about the loss of privacy, the potential for misusing fingerprint information, and the danger of aggregate user profiles being assembled and sold. To avoid the dangers of centralization and unauthorized disclosures, some biometrics developers are considering “one-to-one” matching systems, which use the finger image for corroborative authentication after a user presents a password, PIN, or card. In such systems, a scanner captures a finger image, extracts its features, and converts it into data in the form of a mathematical calculation. The fingerprint data can be

stored on a card. For identification, an individual's captured finger image must match the one stored in the card in the possession of the individual. The only drawback to this form of 1:1 system is that users must carry a card to identify themselves, and this card can be forgotten or lost. The ideal biometric system should not be intrusive and should replace PIN numbers, keys, passwords, and access cards.

DATA SHEET 10.6. WEARABLE COMPUTING SYSTEMS (WCSs)

Developing Critical Technology Parameter	Size; weight; power consumption.
Critical Materials	Thermal management.
Unique Test, Production, Inspection Equipment	None identified.
Unique Software	Real-time operating systems.
Major Commercial Applications	Law enforcement, fire fighting, equipment maintenance, medical, and tactical and special forces.
Affordability	Development of WCSs is based on the integration of COTS components. The true discriminator is size. As size decreases, component cost increases significantly.

BACKGROUND

WCSs consist of head mounted displays (HMDs), non-traditional input/output (NTI/O) devices and low powered, single-board computers. The availability of complete WCSs is driven by commercial consumer product interest. In fact, for approximately \$1,000, a rudimentary WCS can be built with components that are easily assembled, widely available, and come with instructions on the Internet. The component capabilities are increasing rapidly, while size and cost are decreasing.

A WCS is physically always with the individual. It must be extremely lightweight, comfortable, user-friendly, rugged, and unobtrusive and must enhance IP capabilities without hindering other operational tasks. The WCS can exist as a “system of systems” connected via physical wiring or wireless LAN (so-called “body LANs”). Advances in WCS technology are directed toward overcoming the limits of desktop, laptop, or hand-held computers by allowing the user operational mobility. The WCS uses NTI/O, sensors to increase natural remote sensing capabilities with automatic change notification, and instant data access.

SECTION 10.7—INFORMATION SENSING

Highlights

- Proper operation and maintenance of IP and software is highly dependent upon sensor laser test instrumentation and techniques.
- Development in new sensor technology enabling materials is emerging as an important facet of sensor technology assessment.
- Sensor arrays and complex system performance attributes are the products of advanced systems emerging and integration that reduce to practice innovative sensor algorithms, signal processing and software technologies.

OVERVIEW

The Information Sensing FA is defined as capabilities to detect any single or multiple faceted manifestation of properties, qualities, quantities, or other descriptive representations of material or immaterial entities and to produce output signals analogous to the original manifestation sensed—in formats suitable for use in ISs. Entities can be in the form of matter (i.e., exhibiting mass properties, position, motion, chemical, biological, or other characteristics), information, or energy. Considering the wide variety and the different forms in which material and immaterial entities exist in nature, the number of sensor devices or systems needed to determine properties, qualities, and other pertinent characteristics (measurands) of these entities is large. Moreover, because sensor data are used in so many different applications and the requirements for accuracy, resolution, and numerous other parameters are so diverse, the number of measurement technologies, techniques, and products is even larger.

The range of technologies of interest encompasses all categories of sensors and numerous incidences of specific techniques and products.

The Information Sensing assessment for this large field of technology items requires a highly structured and systematic method of addressing the great number of categories, techniques, devices, and systems. To accomplish this, sensors are analyzed first in terms of single, stand-alone devices that normally, or ideally, respond to only a single stimulus or measurand. Next, two classes of sensor arrays or systems are examined. In the first class, “*arrays*” of similar or identical devices are arranged to enhance single measurand detection sensitivity, accuracy, or some other desirable quality. The second class includes a wide range of systems comprising a multiplicity of sensors (possibly dissimilar) or devices, usually deployed to monitor or compare spatial, geographic, temporal, or some other measurand gradation, as opposed to using multiple measurements to enhance sensor quality. The second class also includes the use of dissimilar sensors to detect multiple measurand attributes for one or more entities. For example, to measure kinetic energy, the mass and the velocity of an entity must be determined. Finally, because sensor capabilities are often enabled or constrained by the platforms upon which they are affixed, this subsection addresses important platform-related sensor requirements, capabilities, and corresponding technology solutions. Using examples, Fig. 10.7-1 illustrates this analytical structure and the assessment approach used herein.

In this figure, the right-most column presents a partial listing of measurands associated with solid, liquid and gaseous materials. For most of these measurands, measurements require only a simple or single-device sensor apparatus. Also depicted in this grouping are measurands relevant to atmospheric and other environmental conditions.

The second column from the right depicts measurands associated with non-material entities. This grouping comprises eight kinds of energy,⁸ examples of energy transfer-rates and force, events, and data/information-meaning detection and recognition. The last category includes word/text recognition (e.g., optical character recognition,

⁸ These kinds of energy are defined in *Six Easy Pieces*, Richard P. Feynman, Addison Wesley Publisher.

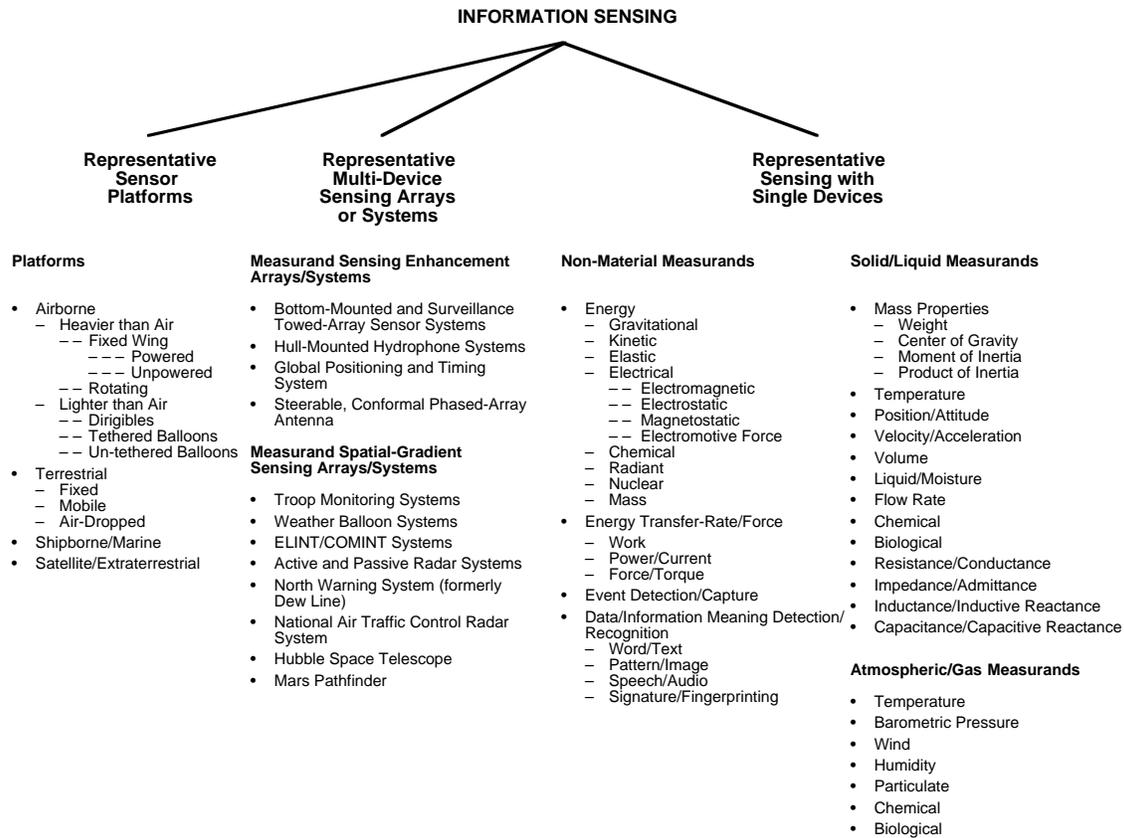


Figure 10.7-1. Information Sensing Taxonomy

text-to-speech synthesis, and so forth), pattern and image recognition, speech recognition, and audio signature detection/ recognition. Described in more detail below, for each measurand listed in the two rightmost columns, there exists a plurality of basic techniques and numerous incidences of vendors and vendor products capable of “sensing” and “measuring” the indicated measurand.

The third column from the right illustrates the multi-device sensor arrays or systems. The first grouping depicts arrays comprised of similar or identical (homogeneous) sensor devices. A classic example of this type of array is the Surveillance Towed Array Sensor System (SURTASS), in which hydrophonic sensors are mounted and spaced along the length of submerged cables and towed by a ship. By combining signals received from each hydrophone, beams are formed in the direction of sound emitters permitting the detection of acoustic energy at distances not possible with single devices. Applications include anti-submarine warfare, oil exploration, and drug interdiction.

An example in the second class of systems using dissimilar sensors or devices is the deployment of large numbers of untethered weather balloons. Such balloons typically carry instrumentation measuring several different meteorological parameters. In this case, the intent is not to improve the quality of any particular parameter measurement, but to monitor or compare spatial or geographic measurand variation.

Finally, the fourth column from the right demonstrates the wide variety of platforms used in sensing operations. When platforms support only sensing missions, they are often designed to optimize sensing operations. When sensor operation is only one of many missions and platform designs cannot be optimized for that purpose, platform-generated interference mitigation and compensation techniques become major sensor technology attributes.

For organizational convenience, most computer system peripheral technologies germane to assessments are, in fact, identified and treated in the tables included in subsection 10.3. Likewise, Section 17, Sensors Technology, addresses many of the complex sensor arrays/systems alluded to previously. Section 17 provides definitional context

for and defines capabilities “unique” to information sensors technologies independent of where they are treated in detail and directs the reader to sections presenting sensor technology assessments.

Most computer system peripherals (i.e., information inputting, outputting, storage and retrieval, printing and publishing, and encoding and decoding devices) are employed in what is most aptly described as information transformation applications. For this reason, as noted previously, the assessment of information transformation technologies, defined as “capabilities to manipulate existing information without changing existing or creating new or extended content or meaning,” is presented in subsection 10.3.

BACKGROUND

Sensing Technology Description

The Information Sensing FA definition at the beginning of this subsection is formulated to apply universally to all incidences of sensing technology. In developing the definition, we found that several authoritative references offered significantly different technical explications of the term “sensor.” For example, the *Department of Defense Dictionary of Military and Associated Terms* (Joint Pub. 1-02) defines a sensor as “an equipment which detects, and may indicate, and/or record objects and activities by means of energy particles emitted, reflected, or modified by objects.”

More elaborately, the *McGraw-Hill Dictionary of Scientific and Technical Terms*, defines a sensor as “the generic name for a device that senses either the absolute value or a change in a physical quantity such as temperature, pressure, flow rate, or pH, or the intensity of light, sound or radio waves and converts that change into a useful input signal for an information-gathering system; a television camera is therefore a sensor; a transducer is a special type of sensor. Also known as a primary detector, sensing element.”

As part of an even more comprehensive definition, the *Communications Standard Dictionary*, by Martin H. Weik, D.Sc., describes a sensor as “equipment that detects the presence or intensity of illumination, radio waves, ionization density, electric fields, or magnetic fields; or equipment that detects the presence of chemicals, such as pollutants and irritants; or the presence of radioactivity. Most detectors are in fact transducers, since they convert energy to another form and amplify it.”

According to these sources, transducers, analog-to-digital (A/D) and digital-to-analog (D/A) converters, other types of converters, and a wide variety of encoder/decoders are legitimate incidences of sensor technology. Consequently, under these definitions, virtually all computer system input/output peripherals are sensors.

To visualize capabilities unique to sensors, consider Fig. 10.7-2. Although the figure uses a thermocouple-based temperature sensor as an example, the distinction between “sensor-unique” capabilities and common metrology, recording, processing, storage, and other general-purpose technology capabilities made here applies to virtually any sensor product or apparatus.

In Fig. 10.7-2, a primary iron-constantan⁹ thermocouple is used to measure the temperature of a gas or some other entity represented by the T_{Hot} symbol. Using primary and secondary thermocouple junctions as shown, an electrical voltage, e_T , is generated. This voltage is directly proportional to the primary thermocouple temperature. In this example, the technology “uniquely” ascribed to the sensor comprises only the thermocouple apparatus and arrangement that results in the generation of the analog voltage, e_T , which is proportional to the entity temperature being measured. From this point on, the figure illustrates both analog and a digital technique, (not “uniquely” designed for sensors) for converting the temperature tracking voltage, e_T , into visible displays for human observation or information that can be processed further and stored by general-purpose computer or process-control equipment.

⁹ An alloy of 45 percent nickel and 55 percent copper, used chiefly in electrical instruments because of its constant resistance.

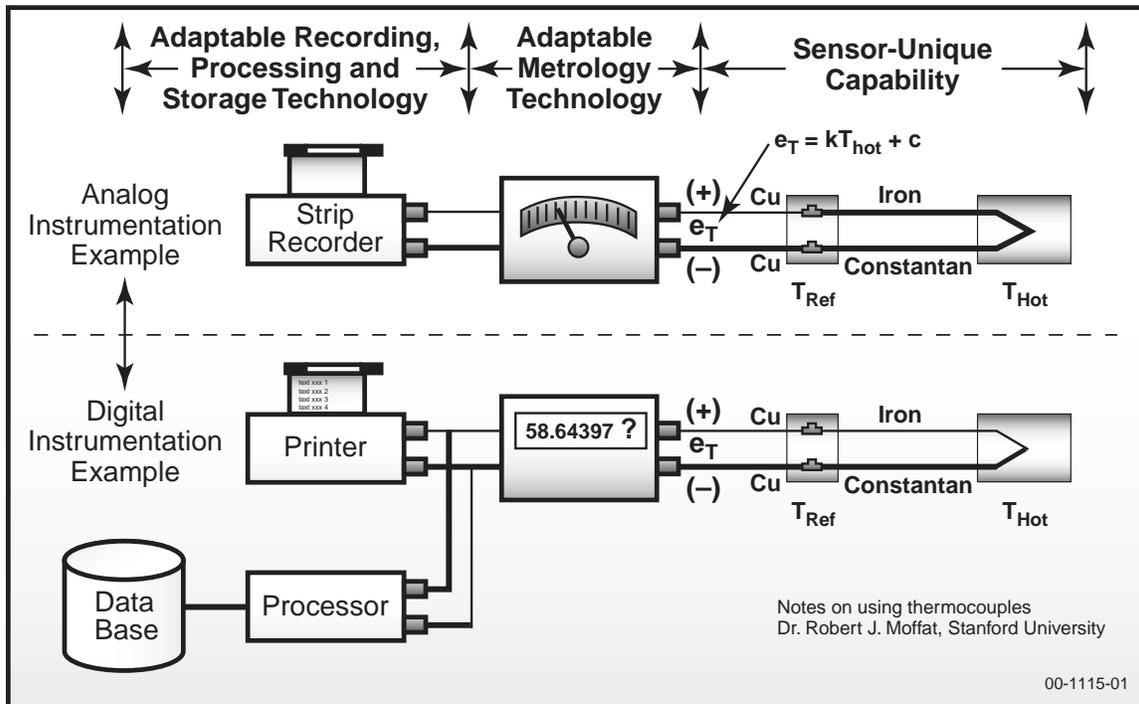


Figure 10.7-2. Thermocouple Example Depicting “Sensor-Unique” Capabilities

While some bimetallic-strip and mercury thermometers directly display temperature readings, in the “analog” approach depicted the top half of Fig. 10.7-2, a “meter” is used to provide visual indication of test-entity temperature. Such meters are typically standard electrical voltmeters with scales calibrated in degrees rather than in volts. The use of COTS strip recorders for continuous time-varying measurement is another example of the adaptation of general-purpose instrumentation in analog sensor equipment. (**Note:** *Subsection 12.3, Metrology, assesses measurement technologies for sensor and other applications.*)

The bottom half of Fig. 10.7-2 presents the digital equivalent of the analog voltmeter and strip-recorder, as well as the possibility of sending digitized temperature data to computers for further processing, storage and future retrieval. Implicit here is an A/D converter to “digitize” the analog, temperature-dependent voltage, e_T .

As noted in extant technical references, because A/D converters can be viewed as “sensing” analog variables and convert them to digital format, they are sometimes defined as sensors in their own right. However, in this example, a fundamental difference between thermocouple action and A/D conversion action is evident. As a “primary” sensor, the thermocouple responds directly to an existing entity condition (a “real” phenomenon—in this case, the actual entity-temperature) and produces information—in analog voltage format—that describes or quantifies that temperature. By contrast, the action of the A/D converter can be described best as simply transforming the thermocouple’s analog output voltage information to information about the same entity-temperature—but in digital format. Although employing A/D converters to “sense” electric potential (an energy-related entity) directly and produce information describing that entity’s magnitude is theoretically possible, A/D converters—in most applications—are used to simply transform information in analog format to the same information in digital format.

Identifying and Assessing “Sensor-Unique” Capabilities

Effective and efficient sensing technology assessment and documentation demands that these efforts focus on “sensor-unique” capabilities—as opposed to technology capabilities that, although essential in sensor operations, are addressed in other assessment activities and sections. Figure 10.7-2 reveals the difference between “unique” primary and adjunct or general-purpose sensor component capabilities in simple, single-device sensors. When assessing primary, single-device technologies, characteristics considered “sensor-unique” include accuracy, resolution, linearity,

cross-measurand measurement distortion, environmental requirements and susceptibilities, stability, repeatability, fungibility, size, weight, volume, reliability, availability, maintainability, and life-cycle cost.

Beyond these technical performance capability considerations, developments in new sensing technology-enabling materials are emerging as another important facet of sensor technology assessment. For instance, fiber-optic-based sensors, which exhibit significant technical performance advantages over electromechanical and chemical predecessors, continue to be introduced for an ever-expanding number of measurands. The following products are now commercially available:

Fiber-Optic-Based Sensor Measurands

Temperature	Chemical Species
Pressure	Force
Flow	Radiation
Liquid Level	pH
Displacement (Position)	Humidity
Vibration	Strain
Rotation	Velocity
Magnetic Fields	Electric Fields
Acceleration	Acoustic Fields

In the domain of sensor arrays and complex systems, “unique” capabilities occur as top-level sensor system functional performance attributes. These attributes are the products of advanced systems engineering and integration techniques that reduce to practice innovative sensor algorithmic, signal processing, and software technologies. Although some aspects of these developments are unique to or developed specifically for sensor systems, to a large extent, they are all implemented by adapting standard or multi-purpose hardware and software configuration items.

In today’s modern SURTASS ocean surveillance sensors, “unique” and standard or multipurpose components are easily identified. In these systems WSC-6 [super high frequency (SHF)] satellite communication (SATCOM) links are used to relay acoustical array information from ships to shore-based processing facilities. Clearly, the common-user WSC-6 communications and the composite theoretical performance (CTP) of shore-based computers, while important to sensor operations, are not the “unique” characteristics of interest in assessing sensor technology.

On the other hand, top-level, SURTASS-unique functional capabilities are sensor unique and, therefore, relevant to sensor technology assessment. Included in this category are all manner of accuracy, resolution, and other effectiveness parameters associated with beam-forming; null steering; automated target detection, identification, and tracking; platform and external noise reduction; ice-thickness measurement; and a myriad of similar system-level performance characteristics.

LIST OF TECHNOLOGY DATA SHEETS
10.7. INFORMATION SENSING

Information Tamperproofing 10-81

The following developing technologies have been identified, but data sheets are not available at this time:

- Data Correlation
- Data Storage and Retrieval
- De-Conflicting Algorithms
- Distributed Database
- Mathematical Modeling of Behavior
- Real-Time Database Updating
- Resource Optimization Algorithms
- Scheduling Algorithms
- Search Engines
- Sensor Tasking Algorithms
- Simultaneous Database Use
- Unstructured Database

DATA SHEET 10.7. INFORMATION TAMPERPROOFING

Developing Critical Technology Parameter	Processing speed.
Critical Materials	None identified.
Unique Test, Production, Inspection Equipment	None identified.
Unique Software	Rapid data storage and processing.
Major Commercial Applications	Law enforcement, financial institutions, historical archives, and news media.
Affordability	Development of algorithms and software is within current technology ability. Cost of additional bandwidth and memory will be low in the 5–25-year time frame.

BACKGROUND

This includes data in almost any format: messages, commands, sensor output, photos, audio recordings, videos, web pages, and real-time transmissions.

Depending on the uses of the data, various levels of tamperproofing protection will be needed.

Some techniques for providing information tamperproofing are possible with current technology. Encryption, user identification, data correlation, consistency checking, and error correction techniques would all be applicable.

SECTION 10.8—INFORMATION VISUALIZATION AND REPRESENTATION

Highlights

- Decision makers will become immersed in their environment by using a 3–D representation, such as holographic imaging or VR capabilities.
- Using visualization and VR, decision makers will not be required to be sophisticated technologically or be expected to initiate or define the details of inquiring methodology.

OVERVIEW

Information visualization and representation is defined as those capabilities employed to view, or make visible, an abstraction of information using physical techniques that include those processing capabilities used to present a data abstraction in a clear and appropriate manner.

In the future, information will be presented in a manner that is easy to comprehend quickly at any level of decision making and in a presentation style chosen by the user. ISs will collect, monitor, and protect information with such accuracy and reliability that the user is confident of the quality of the data representation and accepts it as a basis for decision making.

The underlying ISs will contain an ability to initiate automated self-protection, automated maintenance and repair, and automated disaster detection and recovery. This will be done in a reliable, self-checking and self-deconflicting fashion. When users are presented displays constructed from within an IS, they will have confidence in the validity of these displays.

Data and analytic presentation will be rapid and inexpensive so that multiple users can simultaneously access and inquire about the same information while residing at different locations and using quite different viewer style preferences. Rapid “what-if” analyses will be processed simultaneously, without interference or delay to others engaged in similar inquiry.

BACKGROUND

Decision makers need analytic results of event correlation to be presented in a fashion congruent with their own personal mode of thinking and understanding. Genetic variation creates humans who process information in quite discordant dominant modes and in different combinations of visual, quantitative, or verbal preference. To reduce misunderstanding, ambiguity, or delay in forming a combat decision, data presentation styles will include a selective capability to accommodate those individual preferences. A variety of scenario options that can be explored automatically by the IS and presented in summary form will be available. Decision makers will be able to select and view any desired level of detail upon voice command. Uttering an oral request will modify presentation scale. Analyses will be initiated on request by pointing to a remote graphic, map, chart, or table displayed on a wall using a light-pen or wand.

There may be a need for real-time gathering of information with ongoing specialized analyses, based not only upon requested information but also upon algorithmically derived scenarios offered for optional consideration by the decision maker. The IS will be able to present a projection of the consequences of actions currently being employed and in progress. For example, the viewer could be presented with possible results of the current course of action, based upon automatic algorithmically derived options. This real-time analytic capability does not ensure the outcome, but it does improve a capability to discover errors while sufficient time remains to intervene, recover, or support a stressed force.

In the future, many decision makers will become immersed in their information environment by using a 3–D representation, such as holographic imaging or VR capabilities. The 3–D presentations will be appropriate for use

by individuals and groups. In some situations, robots will be employed to represent individuals acting in a scenario. Individuals will not have to be collocated physically to participate but will appear to other participants in surrogate likeness or simulation. This capability will compensate for situations with personnel limitations.

LIST OF TECHNOLOGY DATA SHEETS

10.8. INFORMATION VISUALIZATION AND REPRESENTATION

Graphics Accelerator Technology	10-85
Virtual Reality (VR) Display Technology	10-86

The following developing technologies have been identified, but data sheets are not available at this time:

- Algorithmically Derived Scenarios
- Change Views
- Coordinated Distributed Activities (Communications, Database Retrieval, and So Forth)
- Cross Section of Images
- Distributed Virtual Reality (VR) Scenarios
- Drill-Down
- Filtering
- Group Virtual Reality (VR)
- Hierarchical Representation
- Holography
- Image Morphing, 2-D and 3-D
- Information Wall
- Network Representation
- Presentation Based on Viewer Style
- Remote Pointing Technologies (e.g., Light-Pen or Wand)
- Training
- Virtual Reality (VR) With Robot Actor
- Voice-Actuated Displays
- White Boarding

DATA SHEET 10.8. GRAPHICS ACCELERATOR TECHNOLOGY

Developing Critical Technology Parameter	Ability to process and generate a dynamic scene at rates exceeding 1.5 Gpixels/sec on a single or multiple display devices.
Critical Materials	None identified.
Unique Test, Production, Inspection Equipment	None identified.
Unique Software	Digital scene generation software and manipulation tailored to model dynamic response of military platforms and sensors.
Major Commercial Applications	Games, entertainment, including interactive digital video disk (DVD).
Affordability	This technology is likely to be driven by mass market products.

BACKGROUND

This technology addresses four closely related functional aspects of displays that are known to affect operator performance: the frame rate, response time, resolution, and fidelity of the representation.

Graphics generators/accelerators represent perhaps the single fastest-advancing segment of the IT market, with performance increasing 8-fold every 18 months. The current state of the art now provides an affordable means of generating stereo imagery at pixel fill rates that approach the requirements for fully immersive systems. However, further advances will probably be needed to realize the level of fidelity and performance needed to support operational military requirements.

The rate of advance of the state-of-the-art is advertised by the industry to be an 8-fold increase in performance every 18 months. One or more of the handful of industry leaders cited brings a new generation to market about every 6 months. The followers in the market tend to trail the state of the art slightly. For example, the current leaders are using 0.18-micron technology, while the followers are in the range of 0.2–0.25 micron technology.

The rapid advance to date has been the result of larger scale application of semiconductor manufacturing. Recent reports are that the Semiconductor Industries Association (SIA) Road Map accelerates the projected availability of 0.13-micron technology.

The availability of state-of-the-art design and fabrication may be a significant factor in the evolution of global capability. The advance of application-specific integrated circuit (ASIC) technology and field programmable gate arrays (which are the basis of the HIPER-KIDS chipset) make the technology accessible. At the same time, the state of the art is clearly being driven by a small number of firms with experience and access to much larger scale VLSI/VHSIC technology.

DATA SHEET 10.8. VIRTUAL REALITY (VR) DISPLAY TECHNOLOGY

Developing Critical Technology Parameter	Ability to match human vision acuity over a field of view exceeding 90 degrees (horizontal) by 70 degrees vertical, with a refresh rate > 100 frames/sec.
Critical Materials	None identified.
Unique Test, Production, Inspection Equipment	None identified.
Unique Software	Digital scene generation software and manipulation tailored to model dynamic response of military platforms and sensors.
Major Commercial Applications	Commercial applications parallel those of the military and tend to fall into high-end dynamic training for aircraft, helicopters, and land and marine vehicles. Advances in the underlying technologies, at the present and for the foreseeable future, are driven by mass-market demand for entertainment and gaming products.
Affordability	At present, systems that begin to approach the levels listed as critical are relatively expensive (\$50,000–\$100,000). Because the technology is being driven by the gaming sector, cost/performance will continue to decline.

BACKGROUND

Two key global trends are likely to have a dramatic affect on the rate at which technology for immersive displays develops over the next five years. The first trend is the rapid advance in graphics accelerators—with performance increasing 8-fold every 18 months. The current state of the art now provides an affordable means of generating stereo imagery at pixel fill-rates that approach the requirements for fully immersive systems. The second trend is the global investment in the development of underlying display materials technologies.

SECTION 10.9—MODELING AND SIMULATION

Highlights

- Modeling and simulation will be used for a wide variety of purposes, e.g., designing, testing and validating systems; game playing.
- Simulators will contain sufficient logic to collect, analyze, and present information automatically and in such a manner that the user will have confidence in the resulting data analyses and representations being presented.
- Many activities are and will be aided by simulation, either to expand the capability of the human user or to replace entirely certain functions previously performed by human users.

OVERVIEW

Modeling is defined here as the mathematical, statistical, or algorithmic representation of real-world aspects that can be used to determine characteristics and parameters of interest. Simulation is defined here as the capabilities of taking on the appearance, form, sound, or other characteristics of some aspect of the real world, most often associated with a time progression when implemented.

In common usage, the term modeling has acquired a wide range of connotation and application. Without constraint or loss of generality, special consideration is given to models described with terms such as theoretical, analytic, stochastic, discrete, continuous, empirical, or deterministic. Provided with a data flow, models can interact with other models, with simulations, or with external objects. Modeling, as an information tool, remains useful across a substantial range of applied and theoretical disciplines that include, but are not limited to, physical, biological, social, and computational systems. Imperfection is a property of every model to the extent that the model fails to replicate the irrational behavior occasionally encountered in humans or physical phenomena not previously observed. Having created a model of appropriate complexity to mirror some object or systemic behavior adequately, one can employ a model for simulation purposes. Basically, simulation exploits a model's structure by constraining selected variables, thus permitting examination of resulting consequences through use of "what if" kinds of inquiry.

Decision making in a military context will continue to require timely analysis based upon disparate, interdependent (although not obviously so) facts arising anywhere in the world. With an increase in the abundance of data flowing into C2 nodes, analysis will require systematic capability and deliberate correlation of data arriving in different formats from many different systems that may have been designed for other purposes. Decision makers are not required to be sophisticated or knowledgeable technologically concerning the details of computational processing. Humans will defer underlying control aspects of information gathering and presentation to systems while retaining active professional judgment, participatory evaluation, and intervention decision choice over any analyses or correlation recommendations presented by the system. Systems of superb design are quite capable of finding unexpected correlation between or among events that seem to share no common or plausible relationship. Since correlation does not imply causality, a careful evaluation of all results presented by any IS remains an essential, active, and participatory function of decision makers at every user level. A system will automatically evaluate a variety of expanding options for presentation in routine formats and selected reports.

M&S will be used for a wide variety of purposes: "what-if" analyses; game-playing analyses; predicting or enumerating likely future action of an opponent; replacing the human interface; and designing, testing, and validating systems. Simulation will aid in enhancing ISs security; managing the systems to optimize efficient use; detecting internal faults and automatically correcting them; scheduling and integrating events; and training personnel. Simulation systems will adapt to the user automatically to provide an appropriate interface while requiring no special user knowledge of the internal workings of the IS on which they are based.

For training purposes, simulation will serve as a productivity enhancement. Simulation will broaden essential skills, maintain skills' currency, and serve to extend organic unit performance capabilities during periods of personnel stress or manpower limitation.

LIST OF TECHNOLOGY DATA SHEETS
10.9. MODELING AND SIMULATION

Behavior Modeling 10-89
Deterministic Modeling 10-89
Discrete Event (DE) Simulation 10-90
Distributed Simulation 10-90

The following developing technology has been identified, but a data sheet is not available at this time:

Data Representation and Visualization

DATA SHEET 10.9. BEHAVIOR MODELING

Developing Critical Technology Parameter	Ability to predict reliably individual and group human performance and response to a realistic range of military situations as a function of any of a number of variables, including fatigue, threat intensity, and physical or psychological stress.
Critical Materials	None identified.
Unique Test, Production, Inspection Equipment	None identified.
Unique Software	Specially designed software and algorithms characterizing human response.
Major Commercial Applications	Significant economic dimensions associated with application of the technology to personnel evaluation, marketing, and effective management of human resources.
Affordability	None identified.

BACKGROUND

The initial objectives of emerging research in this area will be directed toward meeting simulation requirements for realism in computer-generated actors (CGAs). Current models of CGAs depend upon scripted or random actions, which may be only generally related to the current situation as it exists at a given time in the model.

In the near term (5–10-year time frame), the goal is to develop CGAs (individuals and groups) whose behavior will accurately simulate for training purposes the responses that human operators will exhibit when exposed to the same tactical situations. Beyond that time span, further research will be needed to determine whether modeling of human behavior can be made accurate and reliable enough to permit probabilities of actions and behavioral tendencies to be predicted.

DATA SHEET 10.9. DETERMINISTIC MODELING

Developing Critical Technology Parameter	Use of deterministic models to characterize and/or predict performance of complex non-linear systems of multi-element forces in tactical environments.
Critical Materials	None identified.
Unique Test, Production, Inspection Equipment	None identified.
Unique Software	Specially-designed software and algorithms for effective modeling of chaotic behaviors of complex, non-linear systems.
Major Commercial Applications	Significant economic dimensions associated with application of the technology cause a wide range of non-linear systems design problems. Currently, largely an area of academic research.
Affordability	None identified.

BACKGROUND

Visualization and animation techniques have been developed to reduce the complexity and sheer size of the generated data to graphical depictions easily comprehensible by the user. The growing cost of hardware development and test in virtually every product area, coupled with the worldwide availability of low-cost computing power, has made M&S a major area research worldwide.

DATA SHEET 10.9. DISCRETE EVENT (DE) SIMULATION

Developing Critical Technology Parameter	Techniques for distributed parallel modeling of discrete events to permit “faster than real-time” modeling of complex military operations.
Critical Materials	None identified.
Unique Test, Production, Inspection Equipment	None identified.
Unique Software	Software for distribution of discrete event modeling for processing of multiple parallel processors.
Major Commercial Applications	Process control and transportation modeling.
Affordability	None identified.

BACKGROUND

The purpose of a DE simulation is to study a complex system by computing the times and actions that would be associated with events in a real-life situation. While one can carry out a simulation in real time (clock time—the clock on the wall), a DE simulation permits the system to compute, as quickly as possible, the physical times that “still” occur in real time in a physical system, without waiting for the delays between events to occur in real time. Thus, DE modeling lends itself to “faster-than-real-time” simulation, which, in turn, allows the exploration and exercise of multiple scenarios and decision options.

The DE domain provides a general framework for time-oriented simulations of systems such as queuing networks, communication networks, and high-level models of computer architectures. In this domain, events happen at discrete points on the real time line. Each event corresponds to a change of the system state. Each event also has an associated time stamp, which results in a totally ordered set.

- Faster (DE) simulation can be achieved by using dedicated co-processors to speed up event evaluation or control task execution or by developing or improving algorithms and protocols to operate on switched clusters or networks of workstations.

DATA SHEET 10.9. DISTRIBUTED SIMULATION

Developing Critical Technology Parameter	Ability to seamlessly inter-network 1,000 or more real actors and CGAs, with sufficient fidelity and response time so that the actors perceive themselves as interacting in real-time with the actual tactical environment.
Critical Materials	None identified.
Unique Test, Production, Inspection Equipment	None identified.
Unique Software	Software for real-time evaluation and optimization of network and processing tasks designed specifically to implement the M&S HLA and Run-Time Infrastructure (RTI) for military DIS.
Major Commercial Applications	M&S of distributed industrial and business enterprises.
Affordability	Provides major cost savings over traditional field exercises.