DEPARTMENT OF DEFENSE

MILITARILY CRITICAL TECHNOLOGIES

PART III: DEVELOPING CRITICAL TECHNOLOGIES

SECTION 10: INFORMATION TECHNOLOGY

May 2000

Defense Threat Reduction Agency
Dulles, VA

SECTION 10—INFORMATION TECHNOLOGY

Scope

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 Part III, Section 10 will apply herein and in all future MCT publications, including upgrades to the existing Part I and Part II documents.

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.

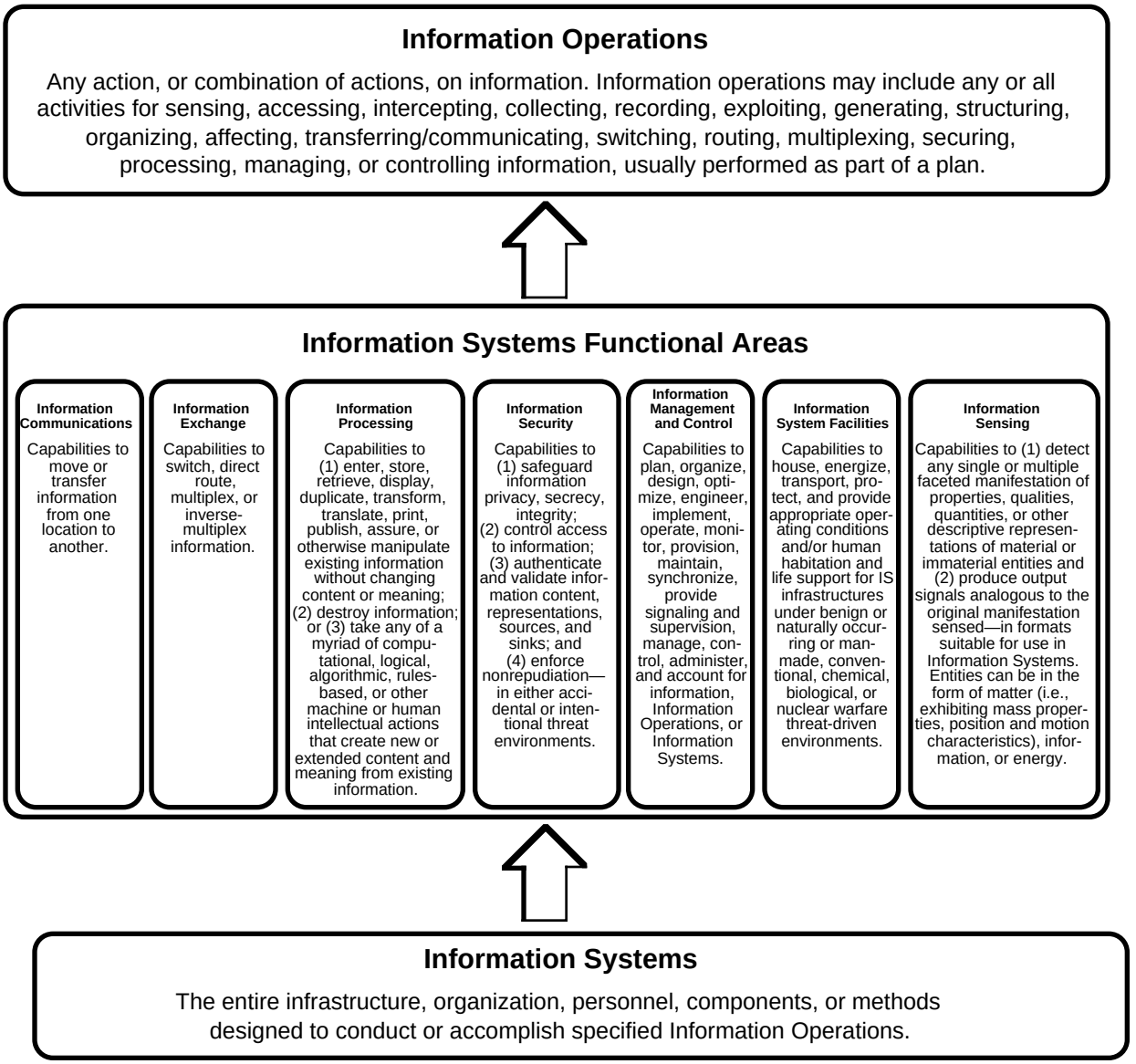


Figure 10.0-1. Information Systems Functional Areas

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 Part III, 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 section (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, ECMs, 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 Figure 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.

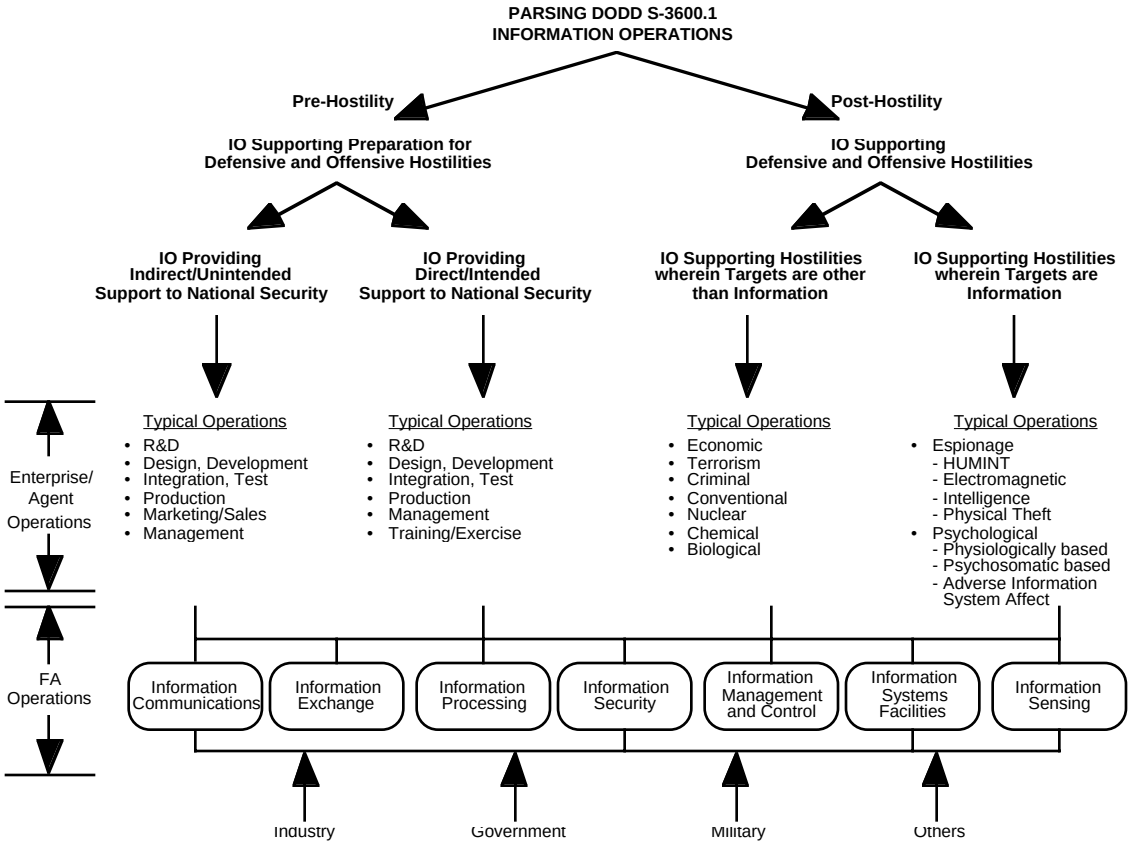


Figure 10.0-2. IO and IS FAs

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 Militarily Critical Technologies (MCT) 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 MCT updates in response to what may be rapidly evolving performance levels of any particular product or technology type. Thus, MCT updates are only required when:

- Changing mission objectives or operational requirements demand corresponding adjustments to "critical" or "sufficient" IT parameter levels (Parts I and II)
- Technological developments advance generic FA performance in ways that enhance the superiority of DoD operations or maintain a superior U.S. capability more affordably (Part III)
- When changes in non-U.S. capabilities necessitate adjustments in Worldwide Technology Assessments (WTAs) (Parts I, II, and III).

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 MCTL Part I 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 for Part III 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 MCT section in which ITs are addressed, the definitions and criteria in this section apply.

RATIONALE

The list of pertinent IOs depicted in Figure 10.0-1 is extensive because long-term National Security really depends upon military and economic parity or superiority and, therefore, is also dependent upon effective, ongoing operations of all supporting industry, government, and military infrastructures. It is axiomatic that a nation must have a solid and sustained financial-economic foundation and, ideally, a position of leadership to become or remain a military superpower. Thus, any and all IOs essential to enterprises critical to a nation's economic health are also essential to its National Security and merit consideration herein.

When the United States was subjected to cold or hot war threats from other military superpowers, it was logical to stress or place a priority on technologies directly related to military crisis or post-hostility operations (i.e., physical, military warfare, and threat-related operations). However, our current decisive military superiority makes it highly unlikely that even technologically advanced third-world nations would be motivated to line up tanks, ships, aircraft, or even missiles against the United States in an all-out, physical military conflict. Rather, a militant and determined third-world adversary bent on hostilities toward the United States is far more likely to expend his resources attacking economic, social, or political targets and, because of the central importance of ISs, attacking IOs

and information itself. Because first- and second-world countries may not possess or be able to mount high-technology INFOWAR/psychological operations-based aggression, the threat that they pose to the United States may be limited to overt or covert economic and geopolitical human operations and acts of terrorism.

The logic then is compelling. At this particular time in history, all adversaries attempting to undermine U.S. economic and military superiority (i.e., those who seek to confiscate, destroy, manipulate, sabotage, or control tangible resources and/or political, military, and civilian organizations) are most likely to target the day-to-day IOs upon which these institutions and resources rely—using their own IO-intensive weapons instead of military force. Moreover, if information is regarded as the basis of technology and technology is the basis for future wealth and economic superiority, the United States is the primary worldwide target since it currently possess the greatest share of economically valuable information.

Perhaps most important to decisions regarding the range and scope of IOs and technologies that must be addressed is this: Not only can INFOWAR be conducted in the total absence of physical conflict, but, unless the United States anticipates such attacks and develops counter technologies to detect and defeat these attacks, our adversaries may be able to mount attacks and achieve victory undetected. This reasoning, however, in no way diminishes the importance of IO superiority as constituent elements of conventional, chemical, biological, and nuclear war-making preparations and capabilities. However, pursuing only those strategies directly linked to physical wartime scenarios ignores the most near-term and dangerous threats to our National Security.

Completing the rationale for the broad spectrum of IOs illustrated in Figure 10.0-2 and addressed herein is recent experience demonstrating the value of military and commercial technologies. Unlike the past where DoD, the National Aeronautics and Space Administration (NASA), and other United States Government (USG) agencies dominated and sponsored most frontier developments, most technologies supporting today's ISs are driven by civil IO requirements and the commercial products responding to those requirements. Thus, we must consider the extensive range of IOs represented in Figure 10.0-2 and the large number of ITs that must be assessed and documented herein.

BACKGROUND

MCTP 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. Although some experts may find even the expanded list of IO activities incomplete, the named activities reflect recommendations of the MCT Information Technology Technology Working Group (TWG).

DODD S-3600.1, Joint Publication 6.0, and past MCTL versions 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 infrastructure, 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 list of MCT 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 tangible 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.*

Existing MCTL versions define "technology" as

> *Specific information and know-how necessary for the development, production, and use of a product. This includes the hardware and software necessary to achieve that purpose.*

Since systems engineering and integration (SE&I) are pivotal in complex IS design and deployment, henceforth, for MCTL purposes, 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.*

WORLDWIDE TECHNOLOGY ASSESSMENT (see Figure 10.0-3)

The WTAs in Section 10 reflect the performance levels that are typically encountered in commercial, military, or non-military government IS technologies and that have been identified in this document as having significant potential in warfighting scenarios. Installed baselines and/or the ability to produce, acquire, and use those technologies are key WTA parameters of interest and are summarized in Figure 10.0-3.

The United States leads in system engineering and integration of complex ISs, closely followed by the Canada, France, Germany, Japan, and the United Kingdom. Underlying technologies for IS and wide area integration of such systems are driven largely by commercial needs and markets. A significant number of countries have developed network switching and transmission capabilities equivalent to those of the United States. The United States has sustained its lead in computer hardware because the it enjoys superior microprocessor design and fabrication capabilities (see Part III, Section 8: Electronics Technology, and this section).

While the United States continues to be the only country with critical capabilities in all IS technology FAs, equivalent capabilities are found in one or more other countries in every FA. The growing multi-nationalization of IS developments has increased the worldwide availability of advanced technologies. IS knowledge transfer from the United States to foreign competitors occurs through open-source U.S. trade journals, technical literature, various international forums, the Internet, commercial competitive analyses, and traditional intelligence services. As a result, the U.S. technology leadership in communications and computer systems has declined in recent years relative to Europe and Japan.

Country	Information Communications	Information Exchange	Information Processing	Information Security	Information Management and Control
Australia	●●●●	●●●●	●●●	●●●●	●●●
Austria	●●●	●●●	●●●	●●●	●●●
Belgium	●●●	●●●●	●●	●●●	●●●
Canada	●●●●	●●●●	●●●●	●●●●	●●●●
China	●●	●●	●●●	●	●●●
Costa Rica	●●	●●	●	●●●	●●
Cuba	●●	●●	●●	●●	●●
Czech Republic	●●	●●	●●	●●	●●
Denmark	●●●	●●●	●●●●	●●●	●●●●
Egypt	●●	●●	●●	●●	●●
Finland	●●●	●●●	●●●	●●●	●●●●
France	●●●●	●●●●	●●●●	●●●●	●●●●
Germany	●●●●	●●●●	●●●●	●●●●	●●●●
Hungary	●●	●●	●●	●●	●
India	●●	●●	●●●	●●	●●●
Iran	●	●	●●	●	●
Iraq	●	●●	●●	●●	●
Ireland	●●●	●●●	●●●	●●●	●●●
Israel	●●●●	●●●●	●●●●	●●●●	●●●●
Italy	●●●●	●●●●	●●●	●●●	●●●
Japan	●●●●	●●●●	●●●●	●●●	●●●●
Libya	●	●	●	●	●
Netherlands	●●●	●●●	●●●	●●●●	●●●●
New Zealand	●●●	●●●	●●●	●●●	●●●
North Korea	●	●●	●●	●	●
Norway	●●●●	●●●●	●●●●	●	●●●●
Pakistan	●	●	●●	●	●●
Poland	●●●	●●●●	●●	●	●●●
Russia	●●●	●●●●	●●●	●●●●	●●
South Africa	●●●	●●●●	●	●●●	●
South Korea	●●●	●●●	●●●	●●●	●●
Sweden	●●●●	●●●●	●●●●	●●●●	●●●●
Switzerland	●●●●	●●●●	●●●	●●●●	●●●
Syria	●●	●●	●●	●	●●
Taiwan - R.O.C.	●●●●	●●●●	●●●	●	●●●
UK	●●●●	●●●●	●●●●	●●●●	●●●●
United States	●●●●	●●●●	●●●●	●●●●	●●●●

Legend: Extensive R&D ●●●● Significant R&D ●●● Moderate R&D ●● Limited R&D ●

Figure 10.0-3. Information Systems WTA Summary

Country	Information Systems Facilities	Information Sensing	Information Visualization and Representation	Modeling and Simulation
Australia	●●●	●	●	●
Austria	●●●●	●	●	●
Belgium	●	●	●	●
Canada	●●●●	●●	●●●	●●●
China	●●	●●●●	●	
Costa Rica	●	●	●	●
Cuba	●●	●	●	●
Czech Republic	●●	●	●	●
Denmark	●●●●	●	●	●
Egypt	●●●	●	●	●
Finland	●●●	●	●	●
France	●●●●	●●●●	●●●	●●●●
Germany	●●●●	●●●●	●●●	●●●●
Hungary	●●	●	●	●
India	●●	●●●●	●	●
Iran	●	●	●	●
Iraq	●	●	●	●
Ireland	●	●	●	●
Israel	●●●	●	●●	●
Italy	●●●	●	●	●
Japan	●●●●	●●●●	●●●●	●●●●
Libya	●	●	●	●
Netherlands	●●●●	●●	●●	●
New Zealand	●	●	●	●
North Korea	●	●	●	●
Norway	●●●●	●●	●	●
Pakistan	●●	●	●	●
Poland	●	●	●	●
Russia	●●●	●●	●	●●●●
South Africa	●	●	●	●
South Korea	●●●	●	●	●
Sweden	●●●●	●	●●●●	●
Switzerland	●●●	●	●	●
Syria	●●	●	●	●
Taiwan - R.O.C.	●●●	●	●	●
UK	●●●●	●●●●	●●●●	●●●●
United States	●●●●	●●●●	●●●●	●●●●

Legend: Extensive R&D ●●●● Significant R&D ●●● Moderate R&D ●● Limited R&D ●

Figure 10.0-3. Information Systems WTA Summary (Continued)

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 hostility.
- 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 reprogrammed for military applications and may achieve levels of survivability far surpassing lower capacity dedicated military systems.
- Long-distance, beyond-line-of-sight (BLOS) communications are essential for remote reconnaissance and damage assessment, aerial strikes launched from one country on targets in an adversary country, and battlefield C2 within large tactical arenas.
- In mixed weapons of mass destruction (WMD) and conventional conflicts, survivable communications are critical to sustaining chemical or biological offensives.

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. This FA includes transmission systems; command, control, communications, computers, and intelligence (C4I) information systems; and aspects of electronic attack and electronic protection.

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 section 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. Allied 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)], videocassette recorder (VCR) video tapes, digital audio tapes, smart cards, and countless others.

Advanced storage technologies (discussed in Section 10.2) that keep physical delivery competitive are impacted by storage and networking technologies. For example, while most personal computer (PC) application software is physically distributed via CD-ROMs, a considerable amount of software can now be downloaded via

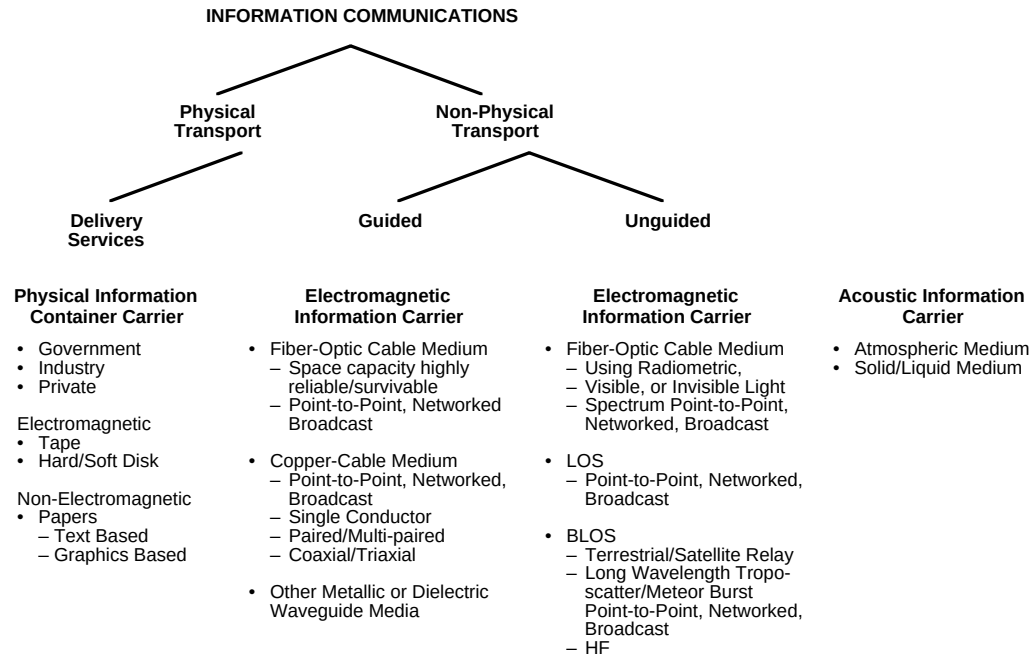


Figure 10.1-1. Taxonomy of INFO COM Technologies

the 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 equality 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 Section 10.3.

Non-Physical Transport

As depicted in Figure 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 include 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 Section 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 section 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 microwaves, 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 a general-purpose microprocessors and software, are listed in the IP FA tables.

RATIONALE

Basic electromagnetic INFO COM requirements can be accomplished using a wide variety of COTS and military-specified products, each with greater or lesser abilities to support military and industrial operations before, during, and after hostilities. Moreover, whether implemented in modern integrated or prior-generation stand-alone products, as indicted below, INFO COM FA capabilities are pervasive in and critical to vital operations of the National Security infrastructure.

INFO COM FA characteristics are important to all National Security infrastructure operations (i.e., critical industry, government, or military operations during pre-, trans-, or post-hostility time frames) and include:

- Global (national and international BLOS or long-distance), near-instantaneous service
- Ultrahigh reliability/survivability
- Mobile or transportable user or operations center connectivity.

Although industry, government, and military organizations depend on these capabilities, industry requirements are typically pursued for business efficiency, competitive advantage, profit, or other largely private economic reasons. Conversely, government—and in particular military—needs are often driven by adversarial threats (physical and otherwise) against life, property, and even the environment itself, with affordability playing a lesser-but-still-vital role. In cases where WMD are factors, hostile environmental conditions may involve chemical, biological, radiation, and electromagnetic pulse (EMP) hazards. Also, on post-hostility time frames, one must anticipate man-made jamming, spamming, or other overt or covert INFOWAR-type attacks to degrade communications environments.

As already noted, the number of situations where unique, military-specified products remain the only option against such attacks is rapidly diminishing. In recent years, the commercial sector has made monumental strides in developing practical, common-user, or public systems yielding ubiquitous, high-reliability, high-survivability, fixed and mobile INFO COM FA capabilities—often at performance levels not achievable with dedicated military facilities. Figure 10.1-1 lists these developments and the rationale describing how and why they relate to the INFO COM FA technologies.

Long-distance communications can be accomplished using cable-based networks, terrestrial or satellite radio relays, long-wave (below 3 MHz/BLOS) radio transmission, or combinations of these techniques. Military long-distance systems can be built from either government-owned, dedicated facilities or shared-facilities obtained

from public or industry-owned common-user networks. Increasingly, modern facilities of either dedicated or shared design are able to provide integrated voice, data, facsimile, imagery, and video services.

At the low-cost end, single-channel long-distance communications can be made today with standard cellular, SMR, or personal communications system (PCS) telephones, interconnected to local and long-distance switched networks. In the near future, end-to-end national and even global mobile voice and narrowband data services will be available form one or more of the following systems: International Marine/Maritime Satellite (INMARSAT), Global Star, ICO Global Communications, Skycell/MobileSat, and ORBCOMM. Broadband satellite-based services, with throughputs on the 2–64 Mbps range, anywhere in the world, are currently planned in the Teledesic, Celestri, and Skybridge programs.

Given an increasing number of efficient mechanisms for long-distance, global communications, the following discussion focuses on the rationale for and emerging technologies that can imbue modern INFO COM capabilities with ultrahigh survivability and reliability operational characteristics. The discourse assesses offensive and defensive requirements from both the United States-allied and adversary-national perspectives.

Requirements for survivability of BLOS military communications arise in strategic and tactical battlefield warfare scenarios. For missile and manned or unmanned aircraft attacks, where the distance between launch points and target designated ground zeros (DGZs) exceeds point-to-point line-of-sight (LOS), there is a need for some form of long-distance communications. Operational situations in which this occurs include aerial strikes launched from one country against targets in another country. Typical targets might include civilian shipping and transportation ports, industrial centers, military command centers, supply depots, and actual battlefield areas. For example, during an ongoing conflict, an aggressor might attempt to create a “plague port” to inhibit an adversary’s ability to receive supplies or debark allied or peacekeeping forces.

BLOS communications are needed to relay information generated by sensors or individuals in the vicinity of the DGZ back to the strike-force headquarters. Such information may include force status reports; micro-meteorological indications and other intelligence data; situation reports; and damage assessment reports. In the near term, voice or low-rate data communications capabilities from ground-based individuals or manned or unmanned airborne reconnaissance platforms may suffice. In the future, sophisticated adversaries may require BLOS communications to relay data from disposable (possibly airdropped), wide-area, array sensors systems.

In-country telecommunications systems with extraordinary availability and survivability can be implemented using emerging commercial fiber- and Synchronous Digital Hierarchy (SDH)-based telecommunications technologies. [In the United States and elsewhere, these systems are built to Synchronous Optical Network (SONET) standards, which, although not identical to International Telecommunications Union (ITU) standards, are equivalent.] Although these systems can ostensibly be procured for peacetime civilian use, with appropriate information exchange switching, multiplexing, and digital cross-connect facilities (see Section 10.2) and information management and control capabilities (IM&C) (see Section 10.5), they can:

- Be reprogrammed for military applications
- Achieve levels of survivability and immunity to physical attack, far surpassing lower capacity, dedicated military designs.

The reason for the extraordinary programmability and survivability of modern commercial telecommunications is twofold. First, the flagship and most profitable telephone carrier offerings today are their “Software Defined Network (SDN)” offerings. SDN allows carriers to offer large customers—who in the past may have opted for private, dedicated facilities-based networks—the option of equivalent “virtual private networks” using the highly redundant and enormous reserve capacity of shared public network facilities. Second, these networks not only offer large industry (or military) customers service indistinguishable from dedicated facilities-based private networks, but they deliver these services at lower cost. Moreover, SDNs greatly augment capabilities to modify, optimize, and customize carrier services, in accordance with changing business or, in times of physical warfare, military requirements.

The reason why modern commercial telecommunications networks are now designed to exhibit unparalleled reliability and survivability is purely economical. For instance, one major U.S. carrier supports the equivalent of 300,000 Washington-to-New York voice circuits. Loss of that connection translates into revenue losses of $30,000 or more per minute. The advent of high-capacity fiber transmission makes it possible to carry an enormous number of voice conversations over a single fiber. Recent advances in wavelength division technology have extended

commercially available fiber-optic capacities to 80 Gbps in a single strand. For the first time in modern telecommunications history, from a reliability-design point of view, this makes possible essentially "free bandwidth." Still, because of the "funnel factor," to ensure profitability and network availability, one must not concentrate that much traffic without adequate back up or redundant connections. Fortunately, SDH/SONET standards addressed this problem from the outset.

In conjunction with automated management and control and appropriate switching and multiplexing facilities, in SDH/SONET networks, this "disposable" bandwidth allows one to design networks that tolerate massive switch and cable-cut failures. In many instances, service restoration is virtually automatic, and restoration is accomplished in 15 ms, a time span short enough to prevent the disconnect of existing calls.

Importantly, use of dual homing and 2 or 4 fiber-based bi-directional line switched ring (BLSR) diversity among switching/multiplexing hubs, along with designed-in capabilities (e.g., embedded SDH/SONET protection routing and automated performance monitoring and diagnostic management functions), yields survivability performance levels that older military systems with precedence, priority, pre-emption, and even dynamic non-hierarchical routing (DNHR) cannot approach. Older techniques preserve or restore service on a call-by-call basis only. By comparison, Sprint has debuted a U.S. network plan for 38 interlocking rings, with 16 nodes per ring, enabling hundreds of thousands of equivalent voice circuits to be restored—almost instantaneously. Since SDH/SONET systems accommodate the world's largest common-user network traffic, bandwidth or channel capacity requirements encountered in military warfare scenarios can be met without employing state-of-the-art switching speeds or ultra-broadband transmission systems.

Satellite-based services are another example of commercial communications offerings exhibiting extraordinary availability and survivability. One class of service providing virtually undeniable service is mobile communications via hundreds of satellites through Teledseic, Globalstar, INMARSAT, and the other systems mentioned previously. Another class of highly reliable and survivable satellite service employs very small aperture terminals (VSATs), which employ small "suitcase-packaged" equipment packages and require antennas of only 1.5–6 ft in diameter. Finally, high-capacity, multi-channel trunk satellite service can be supported with larger-but-still-transportable earth terminals. Not only is it difficult to jam electronically or physically disable the large numbers of satellites providing such services, but to do so would interrupt service to thousands of worldwide users whether or not they are involved in a conflict—a result with potentially enormous negative world-opinion hazards. Thus, for practical purposes, satellite-based communications exhibit dual, BLOS, and equivalent high-survivability capabilities.

Third-world countries are already using satellite services. A case in point is Zambia's presidential limousine that is followed by an INMARSAT satellite-dish-equipped Suburban truck. This provides the president with constant communications connectivity even in rural areas. See Figure 10.1-1 for additional survivable INFO COM technology capabilities with significant enterprise and warfighting potential.

WORLDWIDE TECHNOLOGY ASSESSMENT (see Figure 10.1-2)

Figure 10.1-2 contains a comparative representation of foreign technology assessments (FTAs) for the INFO COM FA by country. All the developed Western nations in the G-8,[1] except for recently joined Russia, plus the Scandinavian countries, Israel, and Taiwan, have capabilities in all elements of the INFO COM FA in their installed base. These capabilities include transmission facilities and required electronic equipment located at nodes along the medium.

Of the G-8, only Russia requires considerable development before it reaches the level of the other members. However, like China, this comparatively late development may be an advantage to Russia because it is not burdened with a large installed base of outmoded analog equipment and bandwidth-limited, non-fiber-optic transmission. Therefore, Russia, China, and other less-developed countries can more readily expand their capabilities with modern equipment, avoiding performance penalties involved with hybrid facilities. The China assessment may be understated since one indicator of China's INFO COM FA capabilities is that the United States alone accounts for up to

1 Canada, France, Germany, Italy, Japan, Russia, the United Kingdom, and the United States,

40 percent of China's exports. Part of this 40 percent, in which China's trade surplus with the United States is greatest, is telecommunications equipment. China manufactures its own fiber-optic cable.

Most other countries with less-developed telecommunications (Cuba, the Czech Republic, Egypt, Hungary, India, Iran, Iraq, Libya, North Korea, Poland, and Vietnam) have fewer INFO COM FA capabilities, and even those tend to be concentrated in larger population centers. However, these deficiencies could be corrected in comparatively short periods. For example, although Iran's telecommunications installed base is concentrated in and around Tehran, Iraq's baseline telecommunications capabilities extend country-wide. See Section 8.11 in Part I of the MCTL.

Country	Physical Transport	Fiber-Optic Cable	Metallic Cable	Line of Sight	Beyond Line of Sight
Australia	●●●●	●●●●	●●●●	●●●●	●●●●
Austria	●●●	●●●	●●●	●●●	●●●
Belgium	●●●	●●●●	●●	●●	●●
Canada	●●●●	●●●●	●●●●	●●●●	●●●●
China	●●	●●	●●	●●●	●●
Costa Rica	●●	●	●	●	●
Cuba	●●	●	●	●	●
Czech Republic	●●	●	●	●	●
Denmark	●●●	●●	●●●	●●●●	●●●
Egypt	●●	●	●	●	●
Finland	●●●●	●●	●●	●●●●	●●●●
France	●●●●	●●●●	●●●●	●●●●	●●●●
Germany	●●●●	●●●●	●●●●	●●●●	●●●●
Hungary	●●	●	●	●	●
India	●●	●	●	●	●
Iran	●	●	●	●	●
Iraq	●	●	●	●	●
Ireland	●●●	●●	●●	●●●	●●●
Israel	●●●●	●●●●	●●●	●●●●	●●●●
Italy	●●●●	●●●●	●●●	●●●●	●●●●
Japan	●●●●	●	●	●	
Libya	●	●	●	●	●
Netherlands	●●●	●●	●●●	●●●●	●●●
New Zealand	●●●	●●	●●●	●●●●	●●●
North Korea	●	●	●	●●	●
Norway	●●●●	●●●	●●●	●●●●	●●●●
Pakistan	●	●	●	●	●
Poland	●●●	●	●	●●●	●●
Russia	●●●	●●	●●	●●●	●●●
South Africa	●●●	●	●	●●●	●●●
South Korea	●●●	●●	●	●●●	●●●
Sweden	●●●●	●●●●	●●●●	●●●●	●●●
Switzerland	●●●●	●●●●	●●●●	●●●●	●●●●
Syria	●●	●	●	●	●
Taiwan - R.O.C.	●●●●	●●●●	●●●●	●●●●	●●●●
UK	●●●●	●●●●	●●●●	●●●●	●●●●
United States	●●●●	●●●●	●●●●	●●●●	●●●●

Legend: Extensive R&D ●●●● Significant R&D ●●● Moderate R&D ●● Limited R&D ●

Figure 10.1-2. Information Communications Technology WTA Summary

LIST OF TECHNOLOGY DATA SHEETS
III-10.1. INFORMATION COMMUNICATIONS

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

Adaptive, Frequency Agile Front Ends [Including Microelectromechanical Systems (MEMS) and Thin Films]
Advanced Coding Technologies
Dynamic Firewall Technology
Low Probability of Intercept (LPI)/Low Probability of Detection (LPD) Waveforms
Message Tracing/Security Technology
Multi-user Detection Technology
Real-Time Conferencing
Smart Antenna Technologies
Software Radio Technologies
Spoofing Detection and Protection Techniques

DATA SHEET III-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- to 38-GHz range.
Unique Software	Software to convert digital bit streams to and from the fiber and the radio.
Technical Issues	This technology should be used in conjunction with code division multiple access (CDMA). CDMA is good in spectrally noisy environments.
Major Commercial Applications	The commercial potential in the United States is the connection of office buildings to the high-speed fiber backbone.
Affordability	This is the most inexpensive way to upgrade current military facilities for the "last mile" and will be much less costly than retrofitting fiber.

RATIONALE

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.

The U.S. military can use this technology for communicating in battlefield or other hostile environments where fiber is not available. For optimal value in the military, this technology depends upon the simultaneous use of CDMA and LEO and using the microwave spectrum between 24 and 38 GHz.

BACKGROUND

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.

In the future, microwave radio transmission is the answer for the military end user. It provides the "missing link" between a high-capacity backbone and the military facility that cannot be served by fiber or would be prohibitively expensive to be served by fiber. High bandwidth and relatively low cost make systems affordable. Also, in many cases, the commercial availability of a provider will allow a system to be set up in several days—if not hours. The short distances and focused beams mean channels can readily be reused without fear of interference—just the thing for military local access.

One of the most promising end-user solutions 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- to 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 to $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.

WORLDWIDE TECHNOLOGY ASSESSMENT

Canada	●●●	Japan	●●●	UK	●●●	United States	●●●●

Legend:	Extensive R&D	●●●●	Significant R&D	●●●	Moderate R&D	●●	Limited R&D	●

Presently the United States leads in this technology roll-out. Europe uses the Global System for Mobile Communications (GSM), which is a variant of time division multiple access (TDMA). GSM is inferior to CDMA. GSM is prevalent everywhere outside North America. The migration of the rest of the world to CDMA should be mostly complete in the 5- to 25-year time frame.

Qualcomm has more than 400 CDMA patents. Globalstar is Qualcomm's CDMA satellite partner. Globalstar is pioneering LEOs for CDMA.

DATA SHEET III-10.1 OPTICAL NETWORKS

Developing Critical Technology Parameter	An all-optical, circuit-switched backbone network will provide abundant, reliable bandwidth.
Critical Materials	High quality fiber cable; erbium doped fiber amplifier (EDFA).
Unique Test, Production, Inspection Equipment	Significantly reduced attenuation fiber at key wavelengths, called AllWave™, is made by only one manufacturer, Lucent.[2] Simple passive filters and waveguides are needed to support wave division multiplexing (WDM). An optical switch is needed for production.
Unique Software	Software to run and configure the optical switches.
Technical Issues	The relatively low number of wavelengths per fiber strand, which is a constraint with other fiber technologies, is much improved with AllWave™ technology because there are more wavelengths available per strand. The need to remove each color of light from the fiber and convert it into an electronic bit stream to amplify and generate the signal every 50 km or so is not a constraint with EDFA. These issues have been solved in early commercial prototypes and installations.
Major Commercial Applications	Anything that communicates digitally.
Affordability	Not an issue. Indeed, an optical network is the lowest cost way to make available large bandwidth for communications. Early military adoption of commercially available resources is not only affordable, but also imminently cost effective.

RATIONALE

Information superiority is the basis for virtually every vision and plan of the U.S. military. Information superiority is attained sometimes by large amounts of data—often by speed of sending or receiving data and information—and always by the reliability of the data and information. More bandwidth is necessary to enable these supporting factors leading to information superiority. Optical network research and development (R&D) represents an eminent future technology for providing more bandwidth, faster throughput service, and greater reliability.

An example of a future military application of reduced attenuation fiber and EDFA to optical networks is the use of these techniques to achieve near-real-time conferencing involving several dispersed physical locations. These future optical network technologies will provide the bandwidth to serve thousands of destinations.

BACKGROUND

WDM and SONET use fiber but with very significant differences. WDM multiplies the capacity of fiber optics by sending messages on many different colors of light—many wavelengths— down the fiber at the same time, allowing a single fiber to bear multiple streams of messages. Having many wavelengths allows communications payloads to be divided into segments that can be more easily managed and manipulated.

If a single wavelength is used, as in SONET, each of hundreds of thousands of messages have to be broken into multiple packets and time slots and coded for reassembly at the other end. Every header in every packet in the flow has to be read to find the packets needed. This approach, acceptable for plain ordinary telephone systems (POTS), performs acceptably for the smaller bandwidths available with copper. However, with the enormous capacity offered by fiber and needed by the military in the future, performing this processing can require the equivalent of

2 AllWave™ is a trademark of Lucent.

a supercomputer, as well as slow and costly transformations from photonics to electronics and back. WDM offers a low-cost and simpler alternative. It promises to break down the bit stream into hundreds of separate message-bearing wavelengths that can be processed by simple passive filters and waveguides.

SONET is good for point-to-point backbone links and giant corporate, government, and university clients in big cities, but it will not serve the military's future large bandwidth needs. SONET will not upscale affordably to provide adequate bandwidth for the U.S. military in the future. To upgrade the SONET bit rate involves prohibitively expensive equipment upgrades and replacements; however, new technologies for WDM will come to the rescue.

In the past, a showstopper for WDM was that every 50 km or so the system would have to remove each color of light from the fiber and convert it into an electronic bit-stream to amplify and regenerate the signal. Each opto-electronic conversion entailed nine expensive bipolar transistors and a host of other devices. However, U.S. commercial companies now have EDFA, which can amplify all the colors at once without having to remove them from the fiber. The contents of the pipe are divided into thousands of wavelengths, each of which can be switched independently with passive optics. If photons do not have to be converted to electrons for regeneration, huge cost savings can be realized on the networks by using passive optical "switches" and converting to electronics and reading packet headers only on the edge of the network in a router on the local area network (LAN). This powerful development will allow an all-optical network, in which messages travel from origin to destination entirely via photons.

For WDM, dividing the contents of the pipe into thousands of wavelengths requires a way of accessing the network that is far less costly than the existing multiplex of opto-electronic converters, packet engines, gold-plated interface cards, and add-drop muxes. With wavelength routing, the perhaps 80 percent of wavelengths that at any given node bear only pass-through traffic can proceed on their way unread, leaving the electronics to manage only the 20 percent of wavelength packets that must be processed. The all-optical network will not switch packets. It will shuffle wavelengths—a much more efficient process.

Now in development by U.S. companies is a product using dispersion management tools and modulation schemes to enable optical signals to travel not 600 km, but 3,200 km. This product uses EDFA technology, which is the final piece of technology to ensure the leap in performance and quality to make feasible the much-increased bandwidth needed in the future. Also, the complex protocols devoted to guarantee "quality of service" at higher levels will be unnecessary. With optical networks, the future outlook is more reliability and more potential capacity with simpler protocols. Available bandwidth is doubling every 3 to 4 months. This projected availability of bandwidth promises to change the face and sometimes the nature of virtually every critical military IT application in the 5- to 25-year time frame.

With millions of times more reliability and more potential capacity than electronics, optical networks largely banish or trivialize all constraints inherited from the electronic networking industry.

WORLDWIDE TECHNOLOGY ASSESSMENT

Canada	●●●	Japan	●●●	UK	●●●	United States	●●●●

Legend:	Extensive R&D	●●●●	Significant R&D	●●●	Moderate R&D	●●	Limited R&D ●

Presently, the United States leads in this technology R&D. Lucent has sought a patent on the AllWave™ manufacturing process. Dow Corning could also have this capability if patent laws and business conditions allow.

Access to the optical network technology is available through U.S. companies. Lucent is the exclusive producers of AllWave™ fiber. Other U.S. companies produce optical cross connects (routers). In the 5- to 25-year time frame, this technology should be in place for the U.S. military. Optical network technology replaces SONET technology and will be much less costly when rolled-out and installed.

DATA SHEET III-10.1. 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.
Technical Issues	Pules position modulation can be used for carrying data. Low-cost, high-performance analog-to-digital converters (ADCs) and digital signal processors (DSPs) are required. Mixed analog/digital circuits are designed for impulse operation rather than sinusoidal operation. Range is short and synchronization acquisition time is long when compared with conventional narrowband radios.
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.

RATIONALE

UWB telecommunications technology supports the warfighter’s capability for dominant battlespace awareness in the Joint Vision 2000 conceptual template. It allows multimode units to be fabricated by combining radar, identification friend or foe (IFF), and communication functions. Current priority is for the development of short-range radar.

UWB technology supports covert radar and space positioning (relative position/location) as well as communications and combat identification (IFF) for squad-level operations. UWB provides relief for frequency allocation problems that are becoming increasingly critical for the military. UWB allows more users per unit of bandwidth and is more efficient in spectral utilization than existing tactical radios.

An applications demonstration system available in the first half of 2000 will have the following characteristics (Ref.1):

- 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 Global Positioning System (GPS) and Federal Aviation Administration (FAA) aeronautical communications (Ref. 2).

W)ORLDWIDE TECHNOLOGY ASSESSMENT

Australia	●	Austria	●	Belgium	●	Canada	●●●
China	●	Finland	●●	France	●●	Germany	●●●
Greece	●	Israel	●	Italy	●	Japan	●●
Norway	●	Russia	●●	Spain	●	Sweden	●
UK	●●●	United States	●●●●				

Legend: Extensive R&D ●●●● Significant R&D ●●● Moderate R&D ●● Limited R&D ●

UWB research is being carried out throughout the industrialized world. At the present time, The United States appears to be the world leader. On November 12, 1999, Siemens Mustang Ventures made a $5-million investment in the Time Domain Corporation to further the development of UWB products. Other are expected to follow (Refs. 3, 4).

The following organizations/individuals have active research programs:

- United States: Aetherwire (Marian County, California), IBM (Burlington, Vermont), Intelligent Automation (Rockville, Maryland), MultiSpectral Solutions (Rockville, Maryland), and Time Domain (Huntsville, Alabama)
- Australia (Eagle & Partners (Victoria)
- Canada: Applanix (Markham, Ontario) and Centraxx (Mississuaga, Ontario)
- Finland: Center for Wireless Communications (Tutkijantie)
- Germany: TEMIC Telefunken (Grossmehring)
- India: Dr. Bhagavathula (Bangalore)
- Israel: Ishay Lev (Mevaseret Zion)
- Italy: Cheechia Systems (Rome) and Mediando Communications (Bologna)
- Netherlands: Parellelweg2 (Groenio)
- New Zealand: IndraNet Technologies (Auckland)
- Russia: Aelita (Moscow).

REFERENCES

1. University of Michigan, *PowerPoint Briefing on Office of Naval Research Communications Technology Program*, 8 February 2000.
2. John Markoff, "FCC Mulls Wider Commercial Use of Radical Radio Technology," *The New York Times*, December 21, 1998, p. C1.
3. William Scott, "Task Force Says Lab's UWB Deals Were Legal," *Aviation Week and Space Technology*, 22 November 1999, p. 50.
4. 1999 International Ultra Wide band Conference Proceedings, http://www.uwb.org/.

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 SDNs that can be used for survivable communications supporting Joint Vision 2010.
- Fast packet, asynchronous-transfer-mode-based switching and multiplexing support voice, data, graphics, imagery, and video requirements.

OVERVIEW

The Information Exchange (INFO EXCH) FA is defined as capabilities to switch, direct, route, multiplex, or inverse-multiplex information. Acting together, systems and equipment implementing INFO COM and INFO EXCH 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, and over links.

Figure 10.2-1 is a taxonomy of the major INFO COM and INFO EXCH system and equipment capabilities that are present in many telecommunications networks. At the highest level in the INFO EXCH category are FA capabilities of “switching” and “multiplexing.”

BACKGROUND

Multiplexing is a technique that enables several communications channels to be combined into a single broadband signal and transmitted over a single circuit. At the receiving terminal, demultiplexing of the broadband signal separates and recovers the original channels. Two basic multiplexing methods used in telecommunications systems are frequency division multiplexing (FDM) and time division multiplexing (TDM).

FDM divides the frequency bandwidth (spectrum) of a broadband transmission circuit into many sub-bands, each capable of supporting a single, full-time communications channel on a non-interfering basis with other multiplexed channels. FDM multiplexing can be used with analog carrier transmission systems. Standard amplitude modulation (AM) and frequency modulation (FM) broadcast radio are examples of FDM, where different stations occupy FCC-assigned portions of the standard broadcast band. Cable television is another example, where different stations are assigned frequency bands on a single cable medium and are selected by appropriate frequency conversion equipment using either stand-alone “converter boxes” or cable-ready television set tuners. In fiber-optic transmission, 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 32-channel systems (80 Gbps) currently possible in the laboratory.

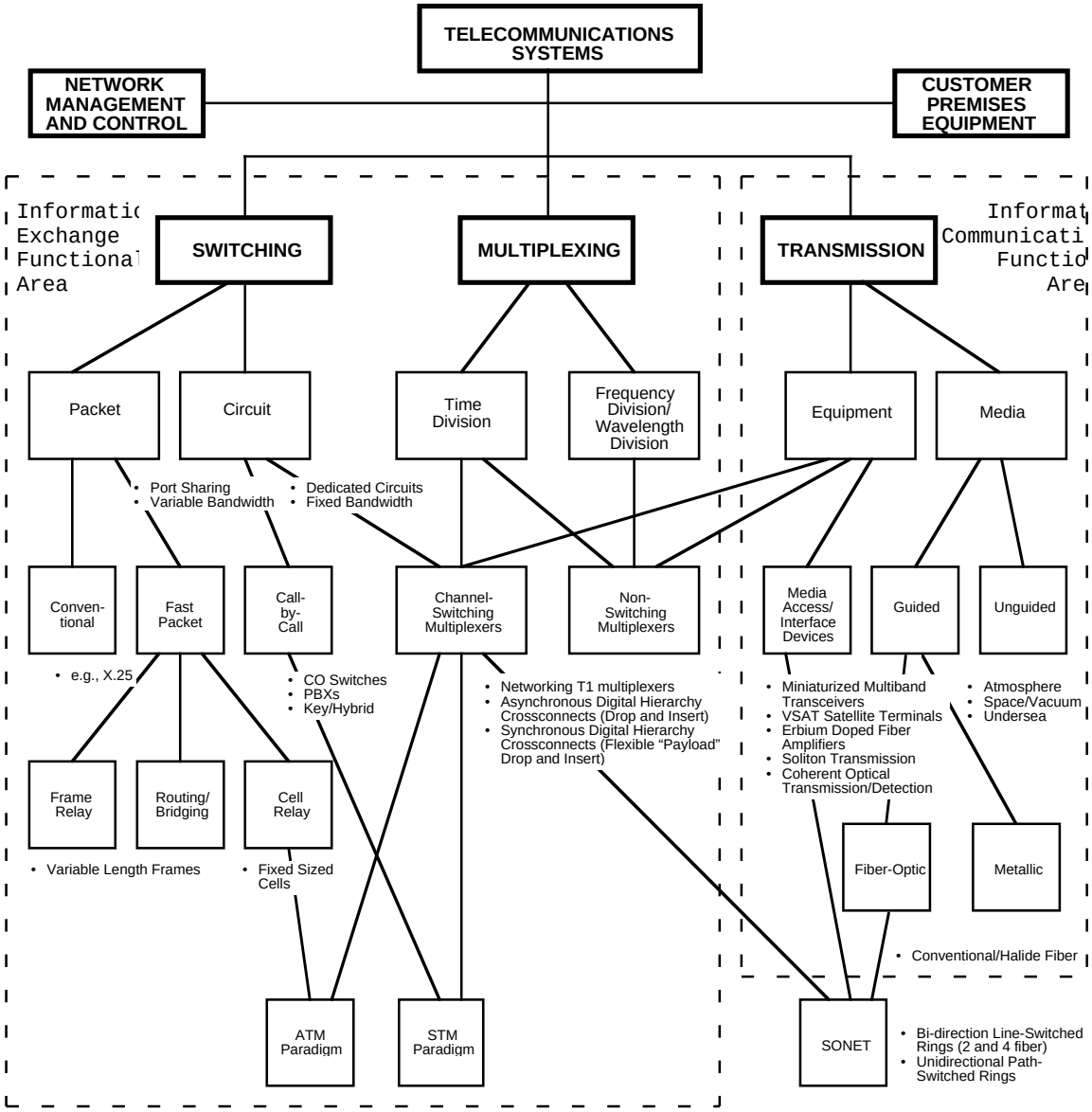


Figure 10.2-1. Taxonomy of INFO EXCH and INFO COM Capabilities

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" TDM was introduced within the old Bell system in which 24 digital voice channels were 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 4,032 digital DS-0 channels and produce 274.176-Mbps signals.

Most modern switch matrix designs use TDM in "time-slot interchange" arrangements. Moreover, nearly all high-capacity switches provide time-division-multiplexed outputs at one or more of the DS-"n" levels. Both of these developments affirm close interrelationships between switching, multiplexing, and the ongoing trends toward even higher levels of equipment and functional integration.

Switching systems interconnect transmission facilities at various network locations and route traffic through a network. Switching includes all kinds of related functions (e.g., signaling, monitoring the status of circuits, translating address to routing instructions, alternate routing, testing circuits for busy conditions, and detecting and recording troubles). As illustrated in Figure 10.2-1, all forms of circuit, packet, and SDH/SONET transport network-based line and path routing and switching are implied. In circuit switching, the INFO EXCH FA encompasses call-by-call [e.g., central office (CO) telephone exchange] and channel switching.

In the past, channel switching was implemented manually at technical control centers. In the United States, by the late 1980s, DCSs began to be installed in 24-channel ("T1," or more properly, DS-1) group-based ADTS. Some DCS equipment provides not only channel switching at DS-1 rates (1.544 Mbps), but also "add and drop" multiplexing without "breaking out" each 64 Kbps DS-0 channel and 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 SDH, ITU G-Series, or SONET-compliant synchronous byte interleave multiplexer equipment. SDH/SONET-based DCS equipment exhibits all basic asynchronous DCS features.

Beyond basic features, SDH/SONET DCSs capitalize on all the considerable advantages of synchronous transmission and multiplexing. Among these advantages is the ability to support synchronous payload envelopes (SPEs) that extend "add and drop" economic and performance advantages across all SDH multiplexing hierarchy levels. In addition, to enhance survivability and availability, SDH/SONET-based BLSRs provide reusable bandwidth for more efficient internode transport in evenly meshed networks.[3]

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. The other half is reserved for protection routing. Thus, in an optical carrier, OC-48,[4] application, working traffic is placed in the first 24 STS-1[5] time slots, with time slots 25 through 48 serving as the protection facility. In conjunction with ITU Telecommunications Management Network (TMN)-based management functions (or vendor product equivalents), this can result in unparalleled recovery from transmission failures—whether these failures occur naturally or from intended or collateral enemy attack damage.

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 DS-3 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 3 minutes—nearly 10 times the number of circuits in 3 percent of the time. See Section 10.5 for a discussion of automated IM&C FA technologies that can lead to this kind of performance in networks used to support military and other missions vital to National Security.

Programmable switching, multiplexing, and computer-based network control technologies alone do not make performance improvements of this magnitude possible. As noted in Section 10.1, with broadband fiber-optic cable and capacity-extending WDM 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 INFO EXCH FA is the wide variety of equipment generally described under the rubric of packet switching. As Figure 10.2-1 shows, packet switching encompasses conventional and fast packet realizations in frame and cell relay appearances. Although 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: 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

---

3 A meshed network means traffic is more or less evenly distributed among all nodes rather than being funneled through a few hubbing locations.

4 OC "n," the "nth" level in an optical carrier multiplexing hierarchy.

5 Sytronic equivalent to OC-1.

common so-called LANs, routers, bridges, switching and non-switching hubs, and numerous satellite access schemes also provide a means for sharing common circuits among multiple traffic channels (multiplexing) and for providing either connection-oriented or connection-less switching functions.

A LAN connects a set of computers to one another across distance via some medium such as twisted pair, coaxial cable, optical fiber, infrared (IR), or radio. Communication from each computer is often first passed to some central command junction, a configuration called a star-wired LAN. That common point, containing a hub or switching system, manages data flow to, from, and among computers connected to the LAN. A hub connection limits its members to some maximum information bandwidth (the number of bits/second the LAN is physically capable of transferring). For example, if a 10-Mbps Ethernet hub were busy handling a 7-Mbps message from one computer, all other computers on the LAN would be collectively slowed as they competed for use of the remaining 3-Mbps-spectrum space. On the other hand, a switch provides each connected computer exclusive use of the full system-designed information bandwidth while providing connections on an as-needed basis.

A router is a device that connects a LAN to one or more than other LANs or to one or more other wide area networks (WANs). Routers forward packets by using their knowledge of the protocols contained within packets. Routers can connect to multiple LANs and WANs and can pass traffic formatted in a variety of protocols. A detailed system configuration defines what actions the router should take in each command instance.

A bridge is a device that connects two separate LANs. A bridge forwards packets of information from one LAN to another, when appropriate, and does so without being concerned for the content or protocol headers contained within the packets. Protocols are communication instruction sets. Since no common standardization of protocols exists across software applications, an “instruction translation” capability has to be included within WAN software. Messages of more than a few hundred bytes are commonly broken down into shorter lengths of numbered packets. Each packet can travel by totally different paths to the final destination where the packets are then reassembled in serial order to recreate the original message. Packeting technology optimizes use of available media resources. Protocols include rules governing how data are structured into packets and sent from one machine to another. A particularly important protocol is the Internet Protocol (IP). Protocols and international standards are constantly evolving.

In addition to the aforementioned switching and integrated switching-multiplexing equipment, equipment assigned to the INFO EXCH FA also includes older non-switching “channel bank” and flexible digital TDMs and all forms of analog electronic and photonic multiplexers (e.g., the modern WDMs).

Each of these LAN and WAN components, supported by appropriate protocols, will have increased capabilities in the future. Routers will evolve to include an extended capability for routing critical military messages. This will be done by using multiple communication capabilities, such as satellite links, moon bounce, passive refraction from orbiting reflectors or meteor ionized trails, very high frequency (VHF) forward tropo scatter, oceanic sub-thermocline paths, and very low frequency (VLF) American Standard Code for Information Interchange (ASCII). Under degraded conditions, this will be done by using aging resident technologies, such as radio teletype (RTTY).

Data compression algorithms will continue to progress, freeing up data bandwidth and reducing transmission time for critical battle content (e.g., topographic maps and imagery). Current text compression methods are sophisticated and reliable. Graphic content has remained somewhat resistant to digital compression techniques that can shrink file size without producing information degradation. Before leaving a site, data are processed through an encryption device. Given sparse assets at any particular location, queuing for crypto processing tends to behave as a significant choke point within the communications operation. Non-destructive compression algorithms will reduce the load on those devices and the generic media load.

Software quality is a critical factor in exchange. Reliable software created by software development methodologies and implemented by trusted, competent developers using rigorous quality control (QC) methods will include intrusion detection as an intrinsic part of the software. Collection of auditing and test data, including that needed for forensic analytic or certification purposes, will be a resident subset of the software and will assist in identifying and removing back-doors, Trojan horse code, and open hooks within software applications.

Software may eventually become reliable enough to protect against external cracking attempts. Crackers usually exploit existing software errors (structural mistakes resident in the delivered product). Counter-cracking technology will evolve so that crackable errors in INFO EXCH computers will be detected and corrected before the

software is installed on a system. These errors are detected during the software certification processes on software developed in trusted or untrusted development environments.

International protocols will gradually become more comprehensive and will support maturing requirements more fully. Full international protocol standardization or convergence to a single protocol set is unlikely because of nationalistic and proprietary propensities. Both software development languages and system design concepts remain dynamic. A decision to tie our systems to any existing protocol set is implicitly a decision to couple our capability to obsolescent technology. Periodic software system upgrades will remain an appropriate solution.

RATIONALE

"Enhancing performance and affordability," the principal criteria for citing MCT Part III technologies, coincides with the fundamental purpose of switching and multiplexing within telecommunications networks, namely, making better and more efficient use of transmission facilities. More specifically, the reasons INFO EXCH FA capabilities are so important to National Security IOs are the same as the reasons they have commercial significance. Quite simply, INFO EXCH capabilities are required as constituent interconnection elements for any IS that extends beyond a "stand-alone" desktop installation. For example, stored program control CO and digital cross-connect switching are key to SDNs. One of the principal advantages of SDNs is that they permit near-real-time network reconfiguration to optimize performance for a wide variety of traffic types and loading or in response to network damage or outages. These same programmability features allow peacetime civilian networks to be converted rapidly to highly survivable communications assets that can support crucial military or civilian disaster operations.

Equally valuable in military or critical industrial operations is the increased accessibility that end-user organizations have to telephone-company-based SDN IM&C facilities that allow them to create and optimize individual subnetworks in accordance with unique customer (or force element) service and configuration profiles. In fact, with the exception of long-wave radio, all BLOS and wide area communications network survivability capabilities described in Section 10.1 depend critically upon INFO EXCH capabilities. Terrestrial or satellite, fixed, cellular, or specialized mobile telecommunications systems are not built without switching and multiplexing. A recent urban warfare study revealed that the Russians in Chechnya, the Israelis in Lebanon, and the British in Northern Ireland resorted to commercial cellular services for mobile troop communications when military-issue portable radio performance proved unsatisfactory within cities.

Operational, Iridium, Teledesic, and other satellite-based capabilities will be even more relevant in satisfying urban mobile communications requirements since the service will involve reduced reliance—or none at all—on indigenous telecommunications facilities. Clearly, all these systems depend critically on highly sophisticated INFO COM, INFO EXCH, and IM&C FA technologies.

Satellite-based mobile telecommunications is one example of commercial technology for which no practical military or government-owned alternative appears to exist. This statement is true unless one wants to defend the position that some country in the world is willing and able to deploy an Iridium or Teledesic-scale satellite constellation for dedicated government-only use. However, although military components are functionally equivalent, these components usually demand higher reliability as measured by a low mean time between failure (MTBF). A combat area is not filtered or air-conditioned. Corrosive explosive residues, vehicle exhaust products, arthropods, mud, water, and dirt are endemic environmental components of battle or of operations in an underdeveloped area.

COTS dual-function switches combining CO and tandem switching capabilities are also available. Thus, in combination with SDH/SONET transmission systems discussed previously, the physical location of switching within a network no longer needs to be fixed or pre-assigned. This results in enormous survivability and service-restoration benefits. In the same vein, dual-function switches also enable a cost-effective means of time-phased upgrading of obsolete telephone systems in urban areas (e.g., Moscow or many third-world metropolitan areas).

Transportable COs used for disaster recovery by telephone companies represent another commercial technology with significant military operations survivability potential. Figure 10.2-1 lists specific INFO EXCH technology capabilities.

WORLDWIDE TECHNOLOGY ASSESSMENT (see Figure 10.2-2)

Figure 10.2-2 contains a comparative representation of FTAs for the INFO EXCH FA by country. The INFO EXCH FA capability profiles of most countries are similar to their INFO COM capabilities. However, some exceptions exist in smaller or less-developed countries. Iraq's, Germany's, Japan's, North Korea's, Russia's, and South Africa's INFO EXCH FA capabilities are assessed as greater than their INFO COM capabilities, whereas Israel's, Poland's, and Taiwan's INFO EXCH FA capabilities are assessed as less than their INFO COM FA capabilities. These lesser INFO EXCH FA capabilities can significantly affect the overall performance of their ISs.

The switching and multiplexing capabilities associated with the INFO EXCH FA are common to military and civil systems and have become readily available through joint developments or foreign sales. The ranking of INFO EXCH FA capabilities largely reflects the effects of international standardization. Australia, Canada, Denmark, Finland, France, Germany, Japan, South Africa, Sweden, Switzerland, and the United Kingdom have overall INFO EXCH FA capabilities equal to those of the United States, although U.S. capabilities may surpass them in some niche technologies (e.g., optical systems). All these countries, plus Italy, sell switching equipment worldwide. In most cases, their export equipment is technologically advanced even though it may incorporate somewhat limited capabilities. For example, their multi-level switching and pre-emption equipment may contain only two levels rather than three to five levels.

Country	Packet Switching	Circuit Switching	TDM	FDM	SONET
Australia	●●●●	●●●●	●●●●	●●●●	●●●●
Austria	●●●	●●●	●●●	●●●	●●●
Belgium	●●●●	●●●●	●●●●	●●●●	●●●●
Canada	●●●●	●●●●	●●●●	●●●●	●●●●
China	●●	●●	●●	●●	●●
Costa Rica	●●	●●	●●	●●	●●
Cuba	●●	●●	●●	●●	●●
Czech Republic	●●	●●	●●	●●	●●
Denmark	●●●	●●●	●●●	●●●	●●●
Egypt	●●	●●	●●	●●	●●
Finland	●●●	●●●	●●●	●●●	●●●
France	●●●●	●●●●	●●●●	●●●●	●●●●
Germany	●●●●	●●●●	●●●●	●●●●	●●●●
Hungary	●●	●●	●●	●●	●●
India	●●	●●	●●	●●	●●
Iran	●	●	●	●	●
Iraq	●●	●●	●●	●●	●●
Ireland	●●●	●●●	●●●	●●●	●●●
Israel	●●●●	●●●●	●●●●	●●●●	●●●●
Italy	●●●●	●●●●	●●●●	●●●●	●●●●
Japan	●●●●	●●●●	●●●●	●●●●	●●●●
Libya	●	●	●	●	●
Netherlands	●●●	●●●	●●●	●●●	●●●
New Zealand	●●●	●●●	●●●	●●●	●●●
North Korea	●●	●●	●●	●●	●●
Norway	●●●●	●●●●	●●●●	●●●●	●●●●
Poland	●●●●	●●●●	●●●●	●●●●	●●●●
Russia	●●●●	●●●●	●●●●	●●●●	●●●●
South Africa	●●●●	●●●●	●●●●	●●●●	●●●●
South Korea	●●●	●●●	●●●	●●●	●●●
Sweden	●●●●	●●●●	●●●●	●●●●	●●●●
Switzerland	●●●●	●●●●	●●●●	●●●●	●●●●
Syria	●●	●●	●●	●●	●●
Taiwan - R.O.C.	●●●●	●●●●	●●●●	●●●●	●●●●
UK	●●●●	●●●●	●●●●	●●●●	●●●●
United States	●●●●	●●●●	●●●●	●●●●	●●●●

Legend: Extensive R&D ●●●● Significant R&D ●●● Moderate R&D ●● Limited R&D ●

Figure 10.2-2. INFO EXCH Technology WTA Summary

LIST OF TECHNOLOGY DATA SHEETS
III-10.2. INFORMATION EXCHANGE

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 III-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.
Technical Issues	Feasibility because of the requirement for high-speed connections.
Major Commercial Applications	Big databases on the Internet; 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.

RATIONALE

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

Many future military applications will require the ability to share large amounts of information. Battle planning and execution require coordination between many dispersed military units, in addition to diplomatic and political input. All the players must be working from coordinated plans and a consistent battlefield view.

BACKGROUND

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 2 and 5 percent of the commercial market, will take it over during the next 5 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. The computer then becomes a series of peripherals attached to the network.

Storage is becoming another abundant commodity. The rapidly collapsing price of storage dictates architectures that waste storage and economize on processing and customer time.

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.

WORLDWIDE TECHNOLOGY ASSESSMENT

Canada	●●●	Japan	●●●	UK	●●●	United States	●●●●

Legend:	Extensive R&D	●●●●	Significant R&D	●●●	Moderate R&D	●●	Limited R&D ●

Presently, the United States leads in this technology implementation.

Microtest pioneered this technology in the early 1990s. Storage area networks (SANs), a transitional step to NAS consisting of multiple storage devices linked by specialized fiber channel hubs and software, are available today from Vixel, Brocade, and Gadzooks. All these are U.S. companies. Network Appliance of Santa Clara, California, is the most aggressive NAS company today. It owns 42 percent of the NAS market. An early adaptation of this technology can be found on mp3.com, which has chosen Network Appliance as their primary storage provider.

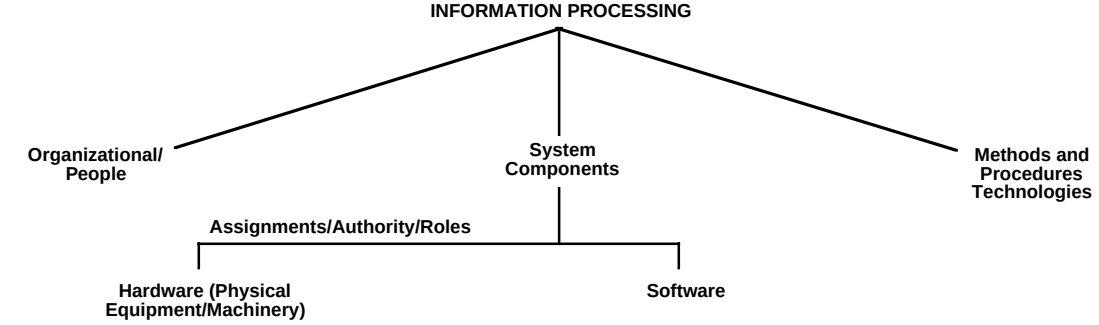
SECTION 10.3—INFORMATION PROCESSING

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.



- Central Processing Units/Microprocessors
  - Arithmetic/Logic
  - Internal Memory
    - – RAM, PROM, EPROM, Flash
  - Control Units
  - Parallel Processing/Symmetrical Multiprocessors
  - Networks or Clusters of Symmetrical Multiprocessors
- External Memory Devices
  - Magnetic
    - – Fixed Single, Multiple, and Array/RAID Hard Drive
    - – Removable Floppy/Diskette
    - – Removable Bernoulli/Cartridge
    - – Conventional/DAT Tape
  - Optical
    - – CD-ROM
    - – Laser Disks/DVD/DIVX
- Input Devices
  - Keyboard/Tablets/Mouse/Pointer
  - Tactical Screen
  - Scanners
  - Voice, Auditory, and other Sensor/Transducer Instrumentation
  - Still and Motion Picture Camera
  - Communications Network
- Ouput Devices
  - Conventional/Holographic Displays and Projectors
  - Printers/Developers
  - Synthetic Voice, Auditory, Visible/Invisible Light, Mechanical, and other Transducers

- Operating System
  - Single/Multiprocessor Computer Operating Systems
    - – Executive
    - – Resource, Device, Communications Network (DE) Inputting, Outputting, and Application Drivers and Controllers
    - – Standards (OLE, DCE, other) Enforcement and Transfer
    - – Administrative and Operational Configuration Controllers
    - – Diagnostic, Recovery, and Maintenance Support
    - – User Services/Options Support
  - Network Operating Systems
    - – Real-Time Network Operations Management and Control
    - – Network Resource Device Drivers and Controllers
    - – Communications Network (DCE) Interface Controllers
    - – Network Traffic and Flow Management, Metering, Recording
    - – Administrative and Operational Configuration Control
    - – Diagnostic, Recovery, and Maintenance Support
    - – User Services/Options Access and Support
- User Application
  - User Work-function/Database Productivity
    - – Text/Word Processing/Hypertext/Mathematical
    - – Drawing/Graphic/Imagery/"N"-dimensional/Hypermedia
    - – On-line Transaction and/or Analytical Processing (OLTP/OLAP)
    - – Flat, Hierarchical, Network, Relational, Object, Intelligent Object
    - – Class/Metaclass/Inheritance Capable, Data Warehousing and Mining Programs
    - – Application-Specific/Integrated Programs
  - Content Cognizant User Conventional and Virtual Reality Interface
    - – Visual/Auditory/Somesthetic/Hard-copy Input-Output
- Language
  - Machine (1 GL), Assembly (2 GL), Procedural (3 and 4 GL), Object (4 GL)
  - HTML, HTL, DDL, DML, and other Standards

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 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 logic[6], 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*.

ISs will manage predefined activities for the user, such as scheduling, recurrent training, flagging events, making case-by-case decisions, and initiating appropriate action. These systemic-level services will remain useful for automating linear logistic flow (e.g., ration quantity levels as troops move into or depart from a battle area) but will not be useful for initiating replacement of non-linearly consumed items, such as bombs, jet fuel, or generic munitions. Underconsumption or unusually high consumption of items will be flagged as will season- or climate-disparate requests (e.g., requisition of parkas for troops in an equatorial area).

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.

RATIONALE

COTS capabilities are intrinsically capable of supporting National Security missions; however, constructing automated strike planning, damage assessment, battle management, sensor and intelligence data fusion, modeling and simulation, weapon inventory and control, and numerous other IP functional capabilities requires significant customization. There is no question that the 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.

Because a transfer of COTS technologies to the IS baseline capabilities does not involve composite material, fuel processing, propulsion system, weapon payload integration, and similar structural and mechanical dependencies, rogue countries (e.g., Iran, Iraq, North Korea, and others) can accomplish a lot at reasonable levels of effort and within aggressive schedules. COTS products [e.g., Internet and Intranet capabilities, distributed computing environments (DCEs), client-server structures, on-line analytical processing (OLAP), and on-line transaction processing

---

6 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.

(OLTP)], a growing family of enterprise software developments, and other commercial developments offer tremendous potential in streamlining and improving WMD and conventional warfare operations.

Multimedia personal power-computers are significant for conflict situations in which transportability and information-supported weapons [e.g., remotely piloted vehicles (RPVs)] are crucial to mission success. High-performance laptop PCs can be conveniently taken to temporary maintenance and repair depots, flight decks, launch vehicles, and battlefields. Slightly larger suitcase-size packaging, augmented with survivable communications and GPS capabilities, extends information-based, warfighting potential even further.

At desktop/workstation capability levels, one can achieve in single-van, transportable command centers what 10 years ago demanded a convoy of vans and support vehicles. This advancement reflects increased IP performance and reliability—all accomplished with greatly reduced computer processor and peripheral size, weight, volume, power consumption and, consequently, scaled-down prime power and environmental control support facilities. Figure 10.3-2 lists specific IP operational capabilities.

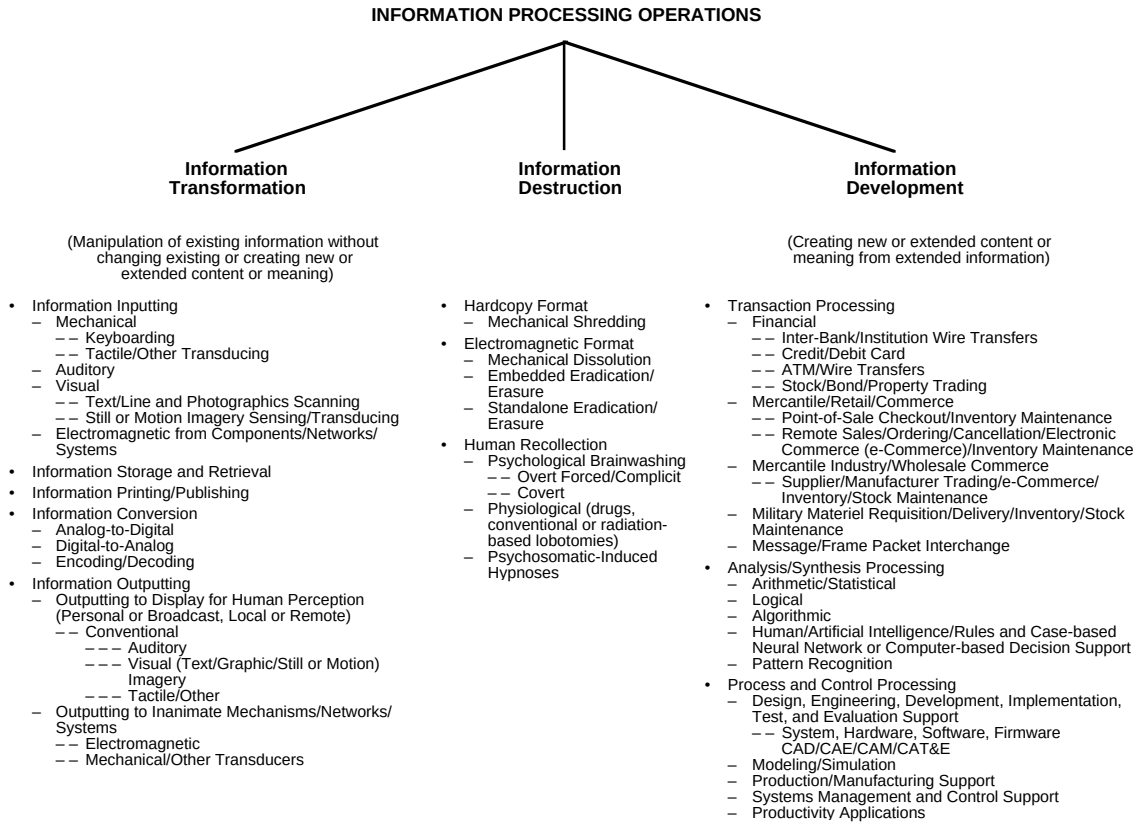


Figure 10.3-2. IP Operational Capabilities

High-performance computing is an enabling technology for modern tactical and strategic warfare. It is the principal technological force multiplier that gives U.S. forces their superior ability to detect, localize, and effectively engage enemy forces in a high threat/target-rich environment. It also enables the processing of massive amounts of imagery and sensor data for real-time data fusion and the generation of synthetic environments for dynamic training and simulation, mission planning and rehearsal, and operational battle management. Embedded computers are key enabling elements for improved sensors and smart weapons; for navigation, guidance, and control of military platforms; and for all aspects of operational command, control, communications, computers, information, and intelligence (C4I2).

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 unstable context presented by a changing set of data. Advanced artificial intelligence (AI)[7] and a subset of expert systems applications will perform well as decision agents or intelligence 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.

WORLDWIDE TECHNOLOGY ASSESSMENT (see Figure 10.3-3)

The United States leads the world in most of these technologies and must continue this lead by a significant margin. U.S. military offensive and defensive capabilities are growing increasingly dependent upon ISs. Being just slightly ahead of other nations risks vulnerability by sustaining an unwarranted overconfidence.

Other countries that contribute to advanced IP research are Canada, Germany, Israel, Sweden, and the United Kingdom. Basic mathematics research is published worldwide, without much constraint. The interval between publication and widespread comprehension may extend for decades. Once understood, mathematics becomes available to all commercial interests, worldwide, for inclusion in their software development. This open flow of emerging IT across borders does not imply that a processing equilibrium or an international parity in system performance will result. Complex and sophisticated software for support of the military will be written by developers who are not constrained by market economics and generic performance specifications that produce so much commercially available software of poor or deceptive quality.

The IP capability profiles of most countries are similar to their INFO COM and INFO EXCH capabilities. However, some significant exceptions exist. India and Iran are assessed as having IP capabilities greater than those capabilities in both their INFO COM and INFO EXCH FAs. Iraq's IP capabilities exceed its IM&C and ISs facilities. Japan, North Korea, and Pakistan have IP capabilities that exceed their INFO COM and INFO EXCH FAs. Only Australia, South Africa, and Switzerland are assessed as having IP capabilities that are less than their INFO COM and INFO EXCH FAs.

Some of the country capability assessments in Figure 10.3-3 may be conservative because the IP capabilities in almost all countries are growing rapidly because of the rapid Internet expansion. IP technology status statistics by country are difficult to locate; however, some indication of various countries' capabilities were revealed by a recent world survey of the Internet host and PC populations. This survey reported that Finland, with a population of 4 million, has the world's largest Internet host density, with ~ 535 per 1,000 population. The United States still leads the world in PC density with ~ 390 PCs per 1,000 population; however, Denmark, Norway, and Switzerland are close behind the United States in PC densities, with more PCs per 1,000 than Canada, Germany, Japan, and the United Kingdom.

Software is changing the economic and military balances in the world. An accelerating intellectual capital transfer of software development know-how is now in progress through the Internet. Intellectual capital transfer takes place through aggressive computer hardware and software marketing, conferences, trade journals, and technical literature on software development and through the graduates of colleges and universities who teach IP skills and

---

7 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.

abilities in the United States and other countries. IP know-how transfer also takes place in personnel transfers overseas and training conducted by U.S. multinational companies. However, the United States still currently leads—and is forecast to continue to lead—the world in software innovation, the development of large complex systems, and system engineering and integration through at least the year 2005 or 2010. The United States has sustained its lead in computer hardware because it enjoys superior microprocessor design and fabrication capabilities. See Sections 5 and 10 in Part I and Sections 8 and 12 in Part III of the 1996 MCTL.

The United States is having a great deal of software developed by foreign nationals, either within their own country or as part of a team in the United States. For example, communications software is being developed in India by a subsidiary of a U.S. communications company. In another case, a critical DoD system being developed under contract in the United States has Russian nationals on the development team. Software developed today is so complex that any programmer(s) could put in viruses, Trojan horses, back doors, and time bombs that could go undetected all the way through installation, particularly if there is a cooperative group effort.

Country	High Performance Computing	Computer Software	Intelligent Systems	Human Systems Interface	COTS Integration
Australia	●●●	●●●	●●●	●●●	●●●
Austria	●●●	●●●	●●●	●●●	●●●
Belgium	●●●	●●●	●●●	●●●	●●●
Canada	●●●●	●●●●	●●●●	●●●●	●●●●
China	●●	●●	●●	●●	●●
Costa Rica	●	●	●	●	●
Cuba	●	●	●	●	●
Czech Republic	●●	●●	●●	●●	●●
Denmark	●●●	●●●	●●●	●●●	●●●
Egypt	●●	●●	●●	●●	●●
Finland	●●●	●●●●	●●●	●●●	●●●
France	●●●●	●●●●	●●●●	●●●●	●●●●
Germany	●●●●	●●●●	●●●●	●●●●	●●●●
Hungary	●	●	●	●	●
India	●●●	●●●●	●●●	●●●	●●●
Iran	●●	●●	●●	●●	●●
Iraq	●●	●●	●●	●●	●●
Ireland	●●●	●●●	●●●	●●●	●●●
Israel	●●●●	●●●●	●●●●	●●●●	●●●●
Italy	●●●	●●●	●●●	●●●	●●●
Japan	●●●●	●●●●	●●●●	●●●●	●●●●
Libya	●	●	●	●	●
Netherlands	●●●	●●●	●●●	●●●	●●●
New Zealand	●●●	●●●	●●●	●●●	●●●
North Korea	●●	●●	●●	●●	●●
Norway	●●●	●●●●	●●●	●●●	●●●
Pakistan	●●	●●	●●	●●	●●
Poland	●●	●●●	●●	●●	●●
Russia	●●●	●●●●	●●●	●●●	●●●
South Africa	●●●	●●●	●●●	●●●	●●●
South Korea	●●	●●●●	●●●	●●	●●
Sweden	●●●	●●●●	●●●●	●●●●	●●●●
Switzerland	●●●	●●●	●●●	●●●	●●●
Syria	●	●●	●●	●●	●●
Taiwan - R.O.C.	●●●	●●●●	●●●	●●●●	●●●●
UK	●●●●	●●●●	●●●●	●●●●	●●●●
United States	●●●●	●●●●	●●●●	●●●●	●●●●

Legend: Extensive R&D ●●●● Significant R&D ●●● Moderate R&D ●● Limited R&D ●

Figure 10.3-3. IP Technology WTA Summary

LIST OF TECHNOLOGY DATA SHEETS
III-10.3. INFORMATION PROCESSING

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

Analytic Recognition of Data Relationships
Data Correlation
Data Storage and Retrieval
Data Warehousing and Mining
Dual Native Language Translation Capability
Dynamic Application Generation
Human Voice Identification
Intelligent Agents
Massive Database Search Algorithms
Native Language Identification Techniques
Search Engines
Unstructured Database

DATA SHEET III-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.
Technical Issues	Key issues are identifying the most effective metaphors for representing different types of large data sets and generating effective algorithms to allow user to manipulate the underlying computational resources.
Major Commercial Applications	Scientific modeling and enterprise modeling operational control, including computer and telecommunications networks, traffic, financial markets, and so forth.
Affordability	No alternative.

RATIONALE

One of the primary goals of Joint Vision 2010 is to achieve and maintain dominant information superiority by giving the commander an overarching perspective and awareness of the battlespace. This will require that the system be able to manipulate and represent the state of readiness and movement of many thousands of individual force elements and their operational capabilities as a function of the state of readiness and battlespace environmental factors.

WORLDWIDE TECHNOLOGY ASSESSMENT

Canada	●●●	France	●●●	Germany	●●●●	Japan	●●●●
UK	●●●	United States	●●●●				

Legend: Extensive R&D ●●●● Significant R&D ●●● Moderate R&D ●● Limited R&D ●

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. The following listing of Centers of Excellence should be considered exemplary but is far from definitive. It focuses on the most frequently cited institutions.

Within the United States, the High Performance Computing Management Office, IBM's Watson Research Center, Xerox, and SGI report substantial corporate research efforts. Georgia Tech University and Carnegie Mellon University (Sage Visualization Group) have broad programs in visualization, and numerous other institutions have efforts aimed at specific visualization applications, very commonly Internet and software development related.

Other frequently referenced centers include:

- Helsinki University of Technology in Finland
- Technical University of Karlsruhe, University of Paderborn, and Dresden University of Technology in Germany
- Computer Sciences Department at the University of Exeter in the United Kingdom.

In Canada, the University of Toronto and the Advanced Computation and Visualization Centre also have efforts aimed at visualization applications. These are two of the six consortia being funded by the Canadian

Foundation for Innovation. Other consortia members include the Memorial University of Newfoundland, University of New Brunswick (Fredericton), University of Prince Edward Island, and St. Francis-Xavier University.

Centers identified in China include Tsinghua University Chinese Academy of Science and the People's University of China.

In France, the Institut National de Recherche en Informatique et en Automatique is the primary focus of computing research. Its five major strategic areas—all of which are related to this topic (the last two directly)—relate to:

1. Control of distributed computer information
2. Programming of parallel machines
3. Development and maintenance of safe and reliable software
4. Construction of systems integrating images and new forms of data
5. Analysis, simulation, control, and optimization of systems.

Japanese industry and academia are heavily involved in data visualization developments. Academic Centers of Excellence include University of Tokyo, Osaka University, and Waseda University.

DATA SHEET III-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.
Technical Issues	Development of effective parallel code and low latency message passing.
Major Commercial Applications	Pervasive.
Affordability	Commodity clusters. USG programs such as the NASA Beowulf and National Institute of Standards and Technology (NIST) initiatives have the explicit goal of making HPC more accessible.

RATIONALE

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.

WORLDWIDE TECHNOLOGY ASSESSMENT

Canada	●●●●	China	●●	France	●●●●	Germany	●●●●
Japan	●●●●	Netherlands	●●	UK	●●●●	United States	●●●●

Legend: Extensive R&D ●●●● Significant R&D ●●● Moderate R&D ●● Limited R&D ●

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. One example of the availability and distribution is the NASA-supported Beowulf program, from which detailed guidance and software for assembling a computing cluster can be accessed and, in the case of the software, downloaded. In the United States, the High Performance Computer Modernization Office (HPCMO) Common High Performance Computing Software Support Initiative (CHSSI) works specifically in the Force Modeling and Simulation (FMS) area, the Defense Advanced Research Projects Agency (DARPA) Cluster is involved in HPC work, the California Institute of Technology/Jet Propulsion Laboratory (JPL) is researching Time Warp development, and NASA funded Synchronous Parallel Environment for Emulation and Discrete-Event Simulation (SPEEDES), a variant of Time Warp.

Because of the increased accessibility of the technology, the number and diversity of activities involved in HPC have increased dramatically. The following paragraphs highlight some specific examples of recognized Centers of Excellence in HPC research.

Canada has a strong initiative in distributed HPC. Nortel, the Canadian telecommunication firm, is a world leader in fiber-optic switching technology, and Canada has established what is advertised as the world's first national optical R&D network, C3.ca, which is a 7-year plan to build a computational infrastructure on a scale that is globally competitive and that supports globally competitive R&D.

Canada's HPC community includes research facilities worth over $70 million. The project will receive $23 million in capital from the Canada Foundation for Innovation. Six universities and regional consortia, which are all C3.ca members, were approved for funding to establish facilities for computation and visualization, including approximately a dozen parallel, shared memory, and vector systems for advanced computing and six new multimedia visualization centers.

Research initiatives of interest to Canadian defense include parallel/distributed intelligent agents, virtual prototyping M&S, and a wide range of software research activities in parallel and distributed computing. Centers of Excellence funded under this effort include:

- High Performance Computing Facility, University of Victoria.
- Multimedia Advanced Computational Infrastructure, University of Alberta.
- University of Calgary, University of Lethbridge, and University of Manitoba. The University of Calgary has conducted many research programs in optimistic parallel processing techniques. It is one of the early and leading HPC research activities.
- Physical Science Computer Network, University of Toronto.
- Interdisciplinary Research Facility for Innovative Applications of Information Technologies, Concordia University.
- Réseau Québécois de calcul de haute performance, Université de Montréal, Centre de recherche en calcul applique, Université de Sherbrooke, with research centers at École polytechnique, McGill University, Université de Québec à Montréal, and Concordia University.
- Advanced Computation and Visualization Centre, Memorial University of Newfoundland, University of New Brunswick (Fredericton), University of Prince Edward Island, and St. Francis-Xavier University.

In France, the Institut National de Recherche en Informatique et en Automatique is the primary focus of computing research. Areas of primary research are organized into five major strategic areas: (1) control of distributed computer information, (2) programming of parallel machines, (3) development and maintenance of safe and reliable software, (4) construction of systems integrating images and new forms of data, and (5) analysis, simulation, control, and optimization of systems.

The German National Research Center for Information Technology oversees and coordinates research in several areas of interest, including basic architecture and software research, autonomous intelligent systems, scientific computing, and distributed collaborative computing. The University of Mannheim, the Technical University of Karlsruhe, and the University of Paderborn are recognized HPC Centers of Excellence.

Collaborative work within Europe is coordinated through the European Research Consortium for Informatics and Mathematics (ERCIM), which aims to foster collaborative work within the European research community and to increase cooperation with European industry. Leading research establishments from 14 European countries are members of ERCIM, whose collaborative activities also extend beyond the European Union (EU). The European Commission has awarded ERCIM a grant to coordinate an EU–China industrial cooperation initiative in HPC. The initiative is also partially financed by the Chinese government through China's National Center for Intelligent Computing (NCIC),[8] with additional funding coming from European and Chinese industry. The goal is to promote Sino–European cooperation by raising Chinese awareness of EU technologies and expertise and to inform the EU business community about market opportunities in China. Participants in relevant Esprit projects will be invited to take part. This High Performance Computing and Networking (HPCN) initiative is part of a range of EU–China industrial cooperation activities in science and technology now being organized under the auspices of the Chinese government and the European Commission.

NCIC's R&D activities in HPC include parallel and distributed computers and carrying out fundamental research on HPCs and intelligent computing systems, especially in the area of natural language interface. While one of NCIC's goals is to develop competitive commercial computer products, results to date appear better suited to

8 The NCIC was founded in March 1990 under the leadership of the Steering Committee of National High-Tech R&D Program (the so-called 863 program) on Intelligent Computing Systems.

developing a fundamental understanding of the underlying technology than to engage in global commercial competition. The “Dawning” family of parallel computing hardware trails the state of the art in terms of its embedded microprocessor and interconnect technologies. However, as research tools, these projects have provided a foundation for investigating effective parallel computing methods.

One area of research that may have military application in coalition warfare and interoperability is the NCIC’s Intelligent Machine Translation Research Center, which is conducting theoretical research, system design, and product development of intelligent machine translation systems.

DATA SHEET III-10.3. QUANTUM INFORMATION PROCESSING/COMMUNICATIONS (QIPC)

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 QIPC systems.
Technical Issues	Ability to control decoherence and perform fault-tolerant operations. Devising suitable methodologies for harnessing decoherence, which would include error correction algorithms, redundancy, and architectural design. Scaling properties in terms of number of qubits, time per gate, and physical size. Developing applications and applications software with commercial markets. Quantum information storage and retrieval, including associated error control. Techniques for initialization of quantum computers, and measurement techniques for efficient read-out of information for internal control and applications. Development of practical repeaters to extend the range of quantum communications.
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.

RATIONALE

Quantum information processing (QIP) holds long-term promise for revolutionary advances in computing, communications, and cryptology. Moore's Law,[9] 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.)

9 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.

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. As noted in the Background section that follows, 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. These capabilities will affect assured services, secure communications, and complete battlespace awareness.

Potential military applications include any in the area now supported by HPC, with unique capabilities in code breaking and secure communications.

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. This suggests potential susceptibility countermeasures that could defeat or degrade such a computer in military applications. 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.

BACKGROUND

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 cryptoanalysis. All public key cryptosystems, which are fused nowadays to protect and to certify electronic documents, will become vulnerable to quantum cryptoanalytic 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.

WORLDWIDE TECHNOLOGY ASSESSMENT

Belgium	●●●	Canada	●●	France	●●●●	Germany	●●●●
Israel	●●	Italy	●●	Netherlands	●●	Japan	●●●●
UK	●●●●	United States	●●●●				

Legend: Extensive R&D ●●●● Significant R&D ●●● Moderate R&D ●● Limited R&D ●

QIPC research is global in nature—with active research efforts in, and collaborative efforts between and among, many different countries. Advances in the underlying science are characterized as revolutionizing the possibilities for processing information on the quantum level. Countries with an evaluation of ●●●● are supported by primary references to specific relevant research and/or multiple citations as Centers of Excellence by other

recognized Centers of Excellence. Lower ratings may be inferred from participation in EU programs or other collaborative efforts, where the specific nature of their contributions is not given explicitly.

Commercial firms with potential to be major developers of QIPC technology include the IBM's Thomas Watson Research Center, British Telecom, Hewlett Packard Laboratories, Thomson CSF, and AT&T Labs. Nippon Telephone and Telegraph (NTT) of Japan has what appears to be a comprehensive effort in quantum optical computing.[10] This list, while not all-inclusive, provides an indication of current interest and shows where the driving impetus for further commercialization may arise.

CENTERS OF TECHNICAL DEVELOPMENT

European Union (EU)

The EU is particularly active in the quantum computing area, with several programs directed toward advancing the state-of-the-art. The ESPRIT-sponsored CERION Working Group will coordinate the research of 17 European and 8 Canadian nodes, actively participating in research on nano-electronics, nano-optics, and the technology of advanced nano-structures. Numerous multilateral efforts are ongoing in the EU, under the Future and Emerging Technologies QIPC Initiative.[11] The Laboratory for Theoretical and Quantum Computing at the University of Montreal is also cited frequently as a center for QIPC research, particularly cryptologic applications.

The goal of the EU QIPC is to develop novel systems and techniques for IP, transmission, and security by exploiting the properties of quantum mechanical operations. The EU initiative presumes that fulfilling these objectives will require many years and numerous projects. Several specific objectives have been defined as guidance and are representative of objectives being pursued in this area, worldwide:

- **Development of an elementary scalable quantum processor.** Although the practical importance of an elementary (e.g., 4-qubit) quantum processor may be limited in itself, it may represent an important step toward larger scale quantum computing.
- **Evaluation and selection of promising component technologies.** To date, all the candidate approaches are affected by rather severe practical limitations. At this juncture, continued exploration of competing approaches (NMR, ion traps, cavity QED, quantum dots, and so forth) and continued research into novel alternative approaches are necessary. Alternatives include the extension of semiconductors and quantum networks that interconnect many simple quantum-processing elements.
- **Quantum algorithm development.** This objective includes the automated discovery of new quantum algorithms. So far, other than in the area of factoring for cryptology and algorithms directed toward quantum mechanical problems, few algorithms tackle problems of practical significance. More applications will be needed to justify future investment.
- **Longer distance and secure quantum communication.** A challenging objective is to scale quantum communication protocols in distance and to demonstrate compatibility with the telecom infrastructure, such as optical fibers. In the area of cryptology, the objectives are to expand quantum key distribution toward longer distances, truly single or entangled photons, multi-party quantum key distribution, and free-space key distribution. The development of quantum key repeaters is seen as an important enabling element of practical communications.

Commercialization of quantum computing technology will ultimately require evolution of an engineering design and development "tool-box" of components, interface standards, and engineering processes that perform specific quantum tasks to be used as building blocks of a QIPC system. Components of interest under the EU QIPC initiative include light sources with controlled fluctuations for photon-based QIPC; non-linear optical fibers for guided photon-pair generation; and coupled semiconductor quantum dots for single-spin or single-photon applications. Examples of quantum engineering processes include quantum measurement techniques, production and use of correlated optical solutions, and quantum interferometry techniques.

---

[10] Nippon Telephone and Telegraph Quantum Optical State Control Research Group, at the web address http://www.brl.ntt.co.jp/physics/butsusei-g/index.html.

[11] European Union Future and Emerging Technologies QIPC Home Page: http://www.cordis.lu/ist/fetqipc.htm.

The following examples shed some light on EU projects that are representative of a much larger overall effort directed toward these areas.

The Centre National de la Recherche Scientifique (CNRS) in Ile de France heads the EU Advanced Quantum Information Research program, in which the France Telecom/Centre National D'etudes de Telecommunications also participates. Other participants in this program are Friedrich-Alexander-Universität Erlangen-Nürnberg and the Universität Konstanz (Germany), Istituto Nazionale per la Fisica della Materia (Italy), Rijksuniversiteit Leiden (Netherlands), and the Defence Evaluation and Research Agency (DERA) (United Kingdom). The Institut Superieur D'electronique Du Nord–Recherche heads the EU effort on scanning tunneling microscope lithography for quantum devices. Other participants in this program are the Université Catholique de Louvain Laboratoire de Microelectronique (Belgium), Instrumat Sa (a French industrial participant), and Omicron Vakuumphysik Gmbh (Germany).

Another EU project in this area is the Spin-Dependent Nano-Electronics, the objectives of which are to combine expertise in semiconductor quantum structures and nano-magnetics to target the field of magnetoelectronics as an important and potentially useful class of quantum devices. Four main objectives are defined:

1. To develop a fabrication technology of mesoscopic magnetic/semiconductor quantum structures by employing the full strength of state-of-the-art nano-fabrication and semiconductor technology, with emphasis on large-scale fabrication and compatibility with integrated circuit (IC) manufacturing
2. To explore the physics and mechanisms of spin-dependent transport in integrated semiconductor/ferromagnetic structures
3. To build optimized devices starting from the three defined concepts: a Vertical Spin Transistor, a Lateral Spin Transistor, and a Magnetically Modulated Semiconductor Transport device
4. To assess magnetoelectronic circuit applications in the fields of non-volatile memory, programmable logic, and reconfigurable input/output circuits, with the first efforts in design and simulation.

This effort is lead by Interuniversity Microelectronics Centre in Leuven, Belgium. Other participants are Thomson CSF (France), Universität Regensburg and Rheinisch-Westfälische Technische Hochschule Aachen (RWTH) (Germany), Weizmann Institute of Science (Israel), University of Twente Mesa Research Institute and University of Groningen (Netherlands), and University of Nottingham and University of Cambridge (United Kingdom).

United Kingdom

The United Kingdom has been active in quantum computing, with major research efforts under way at Oxford, Imperial,[12] Plymouth, Hewlett-Packard Labs, and elsewhere.

The Centre for Quantum Computation, based at the University of Oxford, conducts theoretical and experimental research into all aspects of QIP and into the implications of the quantum theory of computation for physics itself. It is one of the most frequently cited Centers of Excellence for QIPC research.

Quantum cryptography is one part of this field where the United Kingdom has a substantial worldwide lead because of the efforts of researchers at Imperial College (Blackwell Laboratory), Oxford, Strathclyde, DRA Malvern, and BT Laboratories. The basic scientific methodology derives from past activity on non-classical light. Secure quantum communications techniques have been realized in demonstrations. The next step is to use this in network applications.

Germany

German academic institutions are active in the quantum computing area, with ongoing research at the University of Hamburg, the University of Karlsruhe, the University of Bielfield, and the University of Tuebingen. Much of the material cited is available only in German, and German institutions are commonly cited as partners in EU-funded research in this area.

---

12 Simon Bone and Matias Castro, *A Brief History of Quantum Computing*. This site at the Imperial College in London can be found at http://wwwdse.doc.ic.ac.uk/~nd/surprise_97/journal/vol4/spb3/. It contains a good presentation of the history and basic principles of quantum computing, together with an extensive bibliography and links to other useful sites.

Russia

There are reports of Russian work in Quantum Chaos Generation at the Institute for High Performance Computing and Databases in St Petersburg. This research may have potential relevance to quantum computing. Russia, within the Former Soviet Union (FSU), was historically strong in molecular computing. However, the world-leading aspects of this work were primarily in biomolecular computing. Work in optical and quantum nano-electronic devices was, in 1990, assessed to be lagging behind work being done in the United States and Japan.

Japan

Japan is extremely active in QIPC, with work at the University of Tokyo, the University of Kyoto, the University of Osaka, and the University of Hiroshima. Research is reported at Kochi University on "Quantum Computing Solid Block Systems of Nonlinear Dipole-Dipole Ensembles." The NTT Quantum Optical State Control Research Group conducts research across a wide range of topics, all relevant and many directed specifically to future development of QIPC systems. Japanese efforts appear to extend to applications of interest, including work on algorithms at Chiba University and the Science University of Tokyo, and a joint report of research in search and recognition of image data in quantum computers at Kagawa University and Sumitomo Metal Industries, Ltd.

United States

The United States shares or holds world-leading positions in virtually every aspect of quantum computing. There is extensive research in the United States, including the Massachusetts Institute of Technology (MIT), Rutgers University, the Particle Beam Physics Laboratory at UCLA, Stanford University, and dozens of other sites. DARPA and the Army Research Office (ARO) are supporting a MIT/IBM/Stanford NMR computing consortium, which is investigating a wide range of basic topics aimed at moving quantum computing from science to practical engineering. Efforts include synthesis of molecular computers; demonstration of quantum algorithms, including a compiler and algorithms for quantum error correction to control decoherence; scaling investigations, including development of a "desktop NMR quantum coprocessor"; and a 10- to 40-qubit quantum computer.

The California Institute of Technology (Cal Tech) is recognized as a world leader, particularly in techniques for combating decoherence. DARPA is also funding Cal Tech to address specifically potential future military applications of quantum computing. Dr. Neil Gershenfeld at MIT and researchers at the Los Alamos National Laboratory (LANL) are leaders in work toward a concept called "the coffee-cup supercomputer," because of the use of a liquid NMR phenomena. In fact, Dr. Gershenfield believes that a quantum co-processor could be a reality within 10 years if the current pace of advancement continues. Other techniques, such as quantum dots, also show promise.

SECTION 10.4—INFORMATION SECURITY

Highlights

- Information Security (INFOSEC) cryptologic technologies are an increasingly important set of present and future militarily critical technologies (MCTs) 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 3 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 6 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 3 percent. Of the 6 percent of cases resulting from outsider/outside threats, about 3 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 3 percent.

Few commercial, government, or military information systems do not employ technologies cited in this INFOSEC section. 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. Joint Vision 2010 emphasizes the importance of INFOSEC to information superiority by explaining that

There should be no misunderstanding that our effort to achieve and maintain information superiority will also invite resourceful enemy attacks on our information systems. Defensive information warfare to protect our ability to conduct information operations will be one of our biggest challenges in the period ahead. Traditional defensive IW operations include physical security measures and encryption.

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.

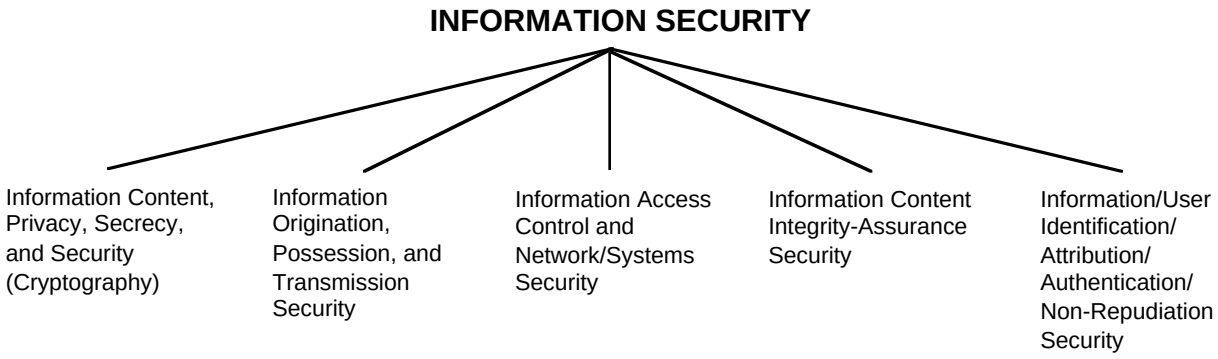


Figure 10.4-1. INFOSEC Applications

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.

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.

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.

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

Offensive Counter-Countermeasures	
Communications Intelligence (COMINT) • Cryptanalytic attacks – Known plain text – Chosen plain text – Chosen cipher text – Brute force	– Protocol – Massively parallel/symmetrical multi-processors – "Black-bag" enhanced • Escrowed encryption • Time/frequency analysis synthesis • Image processing/pattern recognition
Defensive Counter-Countermeasures	
Electromagnetic • Encryption/decryption – Symmetric-key (secret-key) – – 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) – – Factorization – – Discrete log – – Elliptic curve – Mixed symmetric-asymmetric (hybrid)	• Static/dynamic scrambling – Frequency domain – Time domain – Hybrids • Secure non-linear pseudo-noise modulation • Steganography *Physical* • Protected red-enclave • Protected wire distribution • Diplomatic pouch and other protected physical transport • Manual hardcopy encoding/steganography

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.

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 section. However, for organizational reasons, these technologies are discussed in Section 10.6.

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

Offensive Counter-Countermeasures	
Communications Transmission Concealment • Unguided – Electronic signals intelligence/exploitation – – Radio fingerprinting – – Enhanced radiometric detection – Spoofing/communications deception • Guided – Authorized/clandestine wiretapping	*Communications Transmission Assurance* • Unguided – Jamming, spoofing, repeating – – Radio fingerprinting • Guided – Transmission facility sabotage *Counter Operations Security* • Operations Intelligence
Defensive Counter-Countermeasures	
Communications Transmission Concealment • Unguided – Low probability of intercept – Spread spectrum – Low power/duty cycle – Hybrids – Steerable/narrowbeam antennas – Facility/equipment TEMPEST protection • Guided – Protected wire distribution – Fiber-optic/metallic cable *Steganographic Decoy Transmission* *Transmission Assurance* • Unguided – Survivable/anti-jam communications – Spread spectrum – High power – Steerable/narrowbeam antennas	• Unguided/guided – High survivability and availability – Redundant multimedia networks – High reliability fault tolerant designs – Radiation, EMP/HEMP/SGEMP hardened *Operations Security* • Identifying, controlling, and protecting evidence of the planning and execution of sensitive activities • Actions to conceal information origination and/or existence of – Secure compartmented programs – Special access programs – Information, facilities, and equipment

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.

Of greater consequence is adversarial tampering with information content even though this information appears valid to receptors. The attack scenario here is not an enemy trying to deny transmission all together; rather, it is delivering to unsuspecting recipients fraudulent information that appears legitimate.

In many circumstances involving National Security, the satisfactory reception and use of altered, fallacious, and misleading information may be more dangerous than if communications had been denied altogether because it is nearly always true that "falsehood is never so false as when it is very nearly true."[13] The key countermeasure to such information manipulation involves use of secure hash functions.

13 G.K. Chesterton, "St. Thomas Aquinas," 1933.

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

Offensive Counter-Countermeasures	
Espionage • Electromagnetic – 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 – – Public key factoring attacks – – Automated password/war dialer attacks	• Physical hardcopy theft/duplication • Acoustic and visible and Invisible – lightwave activity surveillance *Systems Influence* • System, network, product hardware and software – Operating system, executive, and application software – ASIC • System, network, product hardware and software operational phase sabotage – Remote/networked virus, spoofing, spamming attacks – On-premises hardware and software attacks
Defensive Counter-Countermeasures	
Electromagnetic • Digital certification and authorities • Key management – Key backup and recovery – Key updating and revocation – Key registry and distribution • Network security – Multilevel security – Firewalls, passwords, smart cards – Encrypted management/control and common channel signaling • Systems security – 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	*Steganographic Decoy Transmission* *Transmission Assurance* • Unguided – 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 *Physical* • Tamper-proof packaging • Electronic/physical locks • Protected red enclaves

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.

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

Table 10.4-4. Information Content Integrity-Assurance Security

Offensive Counter-Countermeasures	
Electromagnetic Record Security Counter-Countermeasures • Unguided – Jamming/repeated-signal transmission denial attacks – Deceptive signal transmission attacks • Unguided/guided – Random/deterministic content manipulation – Transmission denial attacks	*Information/Knowledge Accuracy Counter-Countermeasures* • Psychological operations – Philosophically based – Physiologically based – Psychosomatically based • Industrial/financial-economic/scientific disinformation operations • Government/political disinformation operations • Military situation disinformation operations
Defensive Counter-Countermeasures	
Electromagnetic Record Assurance • Error detection and correcting codes • Secure hash functions *Information/Knowledge Accuracy Assurance* • Psychological operations detection/countermeasures – Philosophically based	– Physiologically based – Psychosomatically based • Industrial/financial-economic/scientific disinformation operations • Government/political disinformation operations • Military situation disinformation operations

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

Offensive Counter-Countermeasures	
Information Attribution • Electromagnetic – Counterfeit source/sink/date/container/file location/time-to-user ID attacks • Physical – Counterfeit hardcopy substitution/delivery	*User Identification* • Counterfeit badges/cards • Unauthorized use of user-unique information
Defensive Counter-Countermeasures	
User Identification • Badges/cards/personal identification numbers (PINs) • Smart cards • Biometrics – Thermograms – Hand or eye scanning – Voice printing – Keyboard rhythm – Fingerprint – Signature dynamics	• Digital certification – Digital signature algorithms and techniques *Information Attribution* • Electromagnetic – Source/sink/date/container/file location/time-to-user ID correlation • Physical – Registered/certified mail – Diplomatic pouch/carrier/commercially validated hand delivery

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.

RATIONALE

All the INFOSEC critical developing technologies listed below could support U.S. efforts to achieve and maintain information dominance in future years. The data sheets outline the detailed rationale for including each developing technology.

- Cryptology
- Distributed key generation
- Electronic cash (e-cash) transfer systems
- Elliptic curve cryptosystems
- Hardware-based random number generators
- High-speed encryption
- Image steganography
- Key management
- Key recovery system (KRS) failure mode and effects analyses
- Massively concurrent processor (MCP)
- Message integrity and non-repudiation
- Programmable embeddable communications security (COMSEC)
- Pseudo-random number generation
- Quantum computers
- Quantum encryption
- Secret sharing schemes
- Stream ciphers
- Zero-knowledge proof (ZNP)

For additional information, see the following:

- For an exploration of the idea of developing cryptographic strength metrics, see Annex B to IDA Document D-2121, Addendum to IDA Group Report GR-4 Identification of Militarily Critical Technologies, Part I: Weapons Systems Technologies, Section 8.5: Information Security, December 1997.
- Defense Science Board Task Force Report on Information Warfare-Defense, unclassified version, Executive Summary, paragraph 9.
- For statistics on foreign availability of cryptographic products, visit http://www.tis.com/research/crypoto/crypt_surv.html.
- Testimony by Mr. Stephen T. Walker, President of Trusted Information Systems, for the Subcommittee on Economic Policy, Trade and Environment to the Committee of Foreign Affairs, U.S. House of Representatives, October 12, 1993, p. 8.

TECHNOLOGY ASSESSMENT

Scientific facts are established through open publication of experimental results that may or may not prove to be reproducible in identical peer experiments. The assumption regarding the strength of a cryptographic algorithm is difficult to prove since algorithm strength is based on a belief in the hardness of the solution to the particular mathematical problem on which the cryptography is based. Beliefs are harder to prove than reproducible scientific facts. The strength of a cryptographic algorithm can be established only through open scientific publication that invites peer review. The longer an algorithm is in the public domain and no cryptanalytic solution is found, the greater the cryptographic community confidence becomes that the algorithm is strong and can be trusted. The best way to establish the cryptographic strength of an algorithm is by challenging cryptanalysts—in open publications and on the Internet—to test the strength of the assumption regarding the hardness of the problems on which encryption and algorithms are based. Some developers offer large rewards for those who break their cryptography when testing the strength of their algorithms and providing data for estimating cryptographic life cycles, which are based primarily on processor power and mathematical knowledge.

This period of rapid growth and change in the Information Age is being accelerated by the exponential expansion of the Internet, which has become a world information infrastructure (WII). However, the Internet, like all networks, has also introduced serious vulnerabilities. Exposing the enormous Internet network to "crackers" all over the world has created an exponential market for cryptographic systems to protect National Security information, intellectual property, e-mail, and the e-commerce conducted on the Internet. The international competition among INFOSEC system manufacturers for market share is intense, and the race is on for the shortest-time-to-market and the largest-mind-and-market share for INFOSEC products, all of which incorporate some form of cryptography.

The international demand for INFOSEC products has resulted in an increased rate of acceleration in the critical developing technologies identified in this section. This acceleration is reflected in intense international interest in developing INFOSEC technologies. In recent years, newspapers, trade journals, and technical literature have published a stream of national and international INFOSEC articles and papers about cryptography and cryptanalysis. This rapid rate of change in cryptologic technologies is expected to continue. Until a knee in the Internet growth curve occurs, scientific discovery and technological implementations are likely to lag behind demand. This is especially true for mathematics, elliptic curve cryptographic systems, stream ciphers, image stenography, key escrow or recovery archiving systems, key management, and related infrastructures.

The ensemble of INFOSEC technologies described in this section, if properly designed and combined, comprise defensive countermeasures capabilities that present formidable challenges to those designing or using offensive counter-countermeasures—whether these technologies are implemented with U.S. government/military or COTS products. Although past experience indicates that only 10 percent of information losses are the result of intentional offensive attacks, the ever-increasing use of Internet and Intranets will greatly expand the value of INFOSEC targets. Thus, we can reasonably expect an increase in the absolute number of INFOSEC attacks and in the percentage of losses attributable to them.

Most successful commercial cryptographic systems are based on algorithms in the public domain, which have survived years of peer investigation by the world's best cryptographers. Cryptography is considered to be "strong" by most internationally recognized cryptographers as long as no cryptanalytic technique is discovered that is more efficient than an exhaustive key search. If no short-cut cryptanalytic technique can be found to break the algorithm and if the system equipment and protocols are secure when the algorithm is integrated, the strength of the cryptographic system becomes largely a function of the size of the key space. The longer the key, the stronger the system.

The most important area for improving affordability is the adoption of COTS products to provide protection for sensitive, but unclassified, information. Pilot tests of COTS INFOSEC systems are now underway in various USG departments and agencies. The Internet-driven competition among suppliers should enhance the affordability of the COTS IS security products needed for supporting the national infrastructure assurance for all nations. This competition and the worldwide availability of INFOSEC products should make COTS products better and less expensive in the future. If COTS products can meet military requirements, the adaptation of COTS products could eliminate some of the need for inventory, depots, storage, and related life-cycle support costs. Through standardization, product life might be extended so that new INFOSEC software and hardware are less frequently required—further reducing

replacement costs because of obsolescence and life-cycle costs. A wide selection of competitive COTS products that may meet USG requirements for protecting unclassified sensitive data are already available.

One development that merits further discussion is the growing risk of adversary "system influence" sabotage during the design, development, and manufacturing phases. For instance, massive scale IC technologies now exist to build single chips with 10^8 circuits. Since only a relatively small number of IC input/output pins are available, the ability to embed Trojan Horse-type hardware defects exceeds current abilities to test for such defects. Analogous situations exist in the software regime.

WORLDWIDE TECHNOLOGY ASSESSMENT (see Figure 10.4-1)

In the field of cryptology, the United States has serious competition because more science and mathematics students in many countries are studying cryptology. Cryptology has been studied almost as long (or longer) and intensively in Australia, Canada, France, Germany, the Netherlands, Russia, Sweden, Switzerland, and the United Kingdom as it has in the United States. These and several other countries have world-class cryptographers.

This MCT development cycle has identified other countries that are developing, producing, and distributing commercial cryptography that is as strong as any commercial cryptography developed and produced in the United States. The demand for strong cryptography in the Information Age is growing exponentially with the Internet. In 1993 Congressional testimony, Mr. Walker reported that " . . . we have identified 264 foreign hardware, software, and combination products for text, file and data encryption from 21 foreign countries. . . ." Since 1993, U.S. restrictions on exporting strong cryptography have created a window of opportunity during which foreign cryptographic publishing houses and distributors are increasing their global market share at the expense of U.S. industries. About 4 years later, in December 1997, there were 474 foreign products (up from 264 products in 1993) in at least 68 foreign countries (up from 21 countries in 1993). The reality of the strong foreign commercial cryptographic products, which are widely available in the international market place, increases the value and importance of U.S. cryptology research.

The increasing worldwide cryptologic R&D activity in industry and academia, in response to network requirements for increased INFOSEC and infrastructure assurance, is producing a large body of knowledge that is being published in the open literature. Participation by USG representatives in national and international standards cryptographic technical working groups provides an opportunity to assess and exploit commercial R&D discoveries. The scientific and technological aspects of the state of the art, as well as developing cryptologic technologies and protocols, are often important issues discussed during meetings of national and international INFOSEC standards groups.

Country	Information Content, Privacy, Secrecy, and Security (Cryptography)	Information Origination, Possession, and Transmission Security	Information Access Control and Network/Systems Security	Information Content Integrity-Assurance Security	Information/User Identification/ Attribution/ Authentication/ Non-Repudiation Security
Argentina	●●	●	●	●	●
Australia	●●●●	●	●●●●	●●	●●
Austria	●●●	●	●●	●	●
Belgium	●●●	●	●●●●	●	●
Canada	●●●●	●	●●●●	●	●●
China	●	●	●	●●●	●
Costa Rica	●●●	●	●●●	●	●
Czech Republic	●	●	●●	●	●
Denmark	●●●	●	●●●●	●	●
Finland	●●●	●	●●●	●	●
France	●●●●	●	●●●●	●	●
Germany	●●●●	●	●●●●	●	●
Greece	●	●	●	●	●
Hong Kong	●	●	●	●	●
India	●●	●	●●●	●	●
Iran	●	●	●●	●	●
Ireland	●●●	●	●	●	●
Israel	●●●●	●	●	●	●
Italy	●●●	●	●	●	●
Japan	●●●	●	●	●	●
Korea	●	●	●	●	●
Mexico	●	●	●	●	●
Netherlands	●●●●	●	●	●	●
New Zealand	●●●	●	●	●	●
Norway	●●●	●	●	●	●
Poland	●	●	●	●	●
Portugal	●	●	●	●	●
Russia	●●●●	●	●	●	●
Singapore	●	●	●	●	●
South Africa Rep.	●●●	●	●●	●	●
South Korea	●●●	●	●●●	●	●
Spain	●	●	●	●	●
Sweden	●●●●	●●	●●●●	●●●	●
Switzerland	●●●●	●●	●●●●	●●●	●
Taiwan-R.O.C.	●	●	●	●	●
UK	●●●●	●●●●	●●●●	●●●●	●●
United States	●●●●	●●●●	●●●●	●●●●	●●●●

Legend: Extensive R&D ●●●● Significant R&D ●●● Moderate R&D ●● Limited R&D ●

Figure 10.4-1. Information Security Technology WTA Summary

LIST OF TECHNOLOGY DATA SHEETS
III-10.4. INFORMATION SECURITY

DATA SHEET III-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.
Technical Issues	The integration process will be the principal developmental effort required for military use of this technology. There may also be intellectual property issues. The difficulty in recruiting, training, and retaining cryptologists who are U.S. citizens is a challenge.
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.

RATIONALE

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. Cryptology is used by government and intelligence elements in secure C4IFTW and authentication systems. C4IFTW systems provide hours/days/months of strategic warning to the National Command Authorities (NCA) and minutes/hours of tactical warning. Improved cryptanalysis techniques could be the product of new discoveries in mathematics. Better cryptology will provide increased information superiority and more secure C4IFTW capabilities at lower costs.

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. To ensure access to leading-edge technologies, the United States should provide continuing support for a healthy R&D program in mathematics and cryptology in the USG and at U.S. colleges and universities.

WORLDWIDE TECHNOLOGY ASSESSMENT

Argentina	●●	Australia	●●●●	Austria	●●●	Belgium	●●●
Canada	●●●●	China	●	Costa Rica	●●●	Czech Republic	●●
Denmark	●●●	Finland	●●●	France	●●●●	Germany	●●●●
Greece	●	Hong Kong	●	India	●●	Iran	●
Ireland	●●●	Iraq	●	Israel	●	Italy	●
Israel	●●●●	Italy	●●●	Japan	●●●	Korea	●
Mexico	●	Netherlands	●●●●	New Zealand	●●●	Norway	●●●
Poland	●	Portugal	●	Russia	●●●●	Singapore	●
South Africa Rep.	●●●	South Korea	●●●	Spain	●	Sweden	●●●●
Switzerland	●●●●	Taiwan-R.O.C.	●	UK	●●●●	United States	●●●●

Legend: Extensive R&D ●●●● Significant R&D ●●● Moderate R&D ●● Limited R&D ●

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. Some of the prominent producers of mathematics based cryptologic systems are:

- Canada: Entrust [Nortel] and Certicom
- United States: RSA Data Security, Inc., [Security Dynamics], Cylink, IBM, Motorola, CertCo, BBN Technologies [GTE], Fischer International, and TIS.

There are many more U.S. companies and over 700 foreign cryptographic products for sale in the world market for text, file, and data encryption.

DATA SHEET III-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.
Technical Issues	No development—other than the promulgation of standards and integration into existing applications—should be required for the military use of COTS public key systems that provide distributed key generation. Intellectual property rights may encumber this technology. A ubiquitous directory infrastructure is required for certificates and related information.
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.

RATIONALE

Distributed key generation is fundamental to meeting the requirement for secure, scaleable cryptographic systems. It is a basic requirement for security products designed for use in large, distributed C4IFTW environments. The civilian sector already 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 (see Chairman, Joint Chief of Staff's *Joint Vision 2010*, the U.S. Army's FM 100-6, *Information Operations*, and the U.S. Air Force's *New World Vistas: Air and Space Power for the 21st Century*).

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. Secure C4IFTW systems could provide hours/days/months of secure strategic warning to NCA and minutes/hours of secure tactical warning to battlefield commanders.

WORLDWIDE TECHNOLOGY ASSESSMENT

Australia	●●	Belgium	●	Canada	●●●●	France	●
Germany	●	India	●	Ireland	●●	Israel	●●●●
Italy	●	Japan	●	Netherlands	●●●	New Zealand	●
Russia	●●●	South Africa Rep.	●	Sweden	●●	Switzerland	●●
UK	●●●●	United States	●●●●				

Legend: Extensive R&D ●●●● Significant R&D ●●● Moderate R&D ●● Limited R&D ●

Governments are developing dual-use distributed key generation and PKI systems. In the United States, military development programs include distributed key generation and public key features. Commercial developers already produce public key system products that support distributed key generation. National and international standards organizations are, in fact, the principal centers of PKI protocol development. Some of the principal producers of cryptographic public key systems that support distributed key generation are:

- Canada: Entrust [Nortel] and Certicom
- United States: RSA Data Security, Inc., [Security Dynamics], Cylink, IBM, Motorola, CertCo, BBN Technologies [GTE], Netscape, Spyrus, TIS, VeriSign, and Xcert [Fischer International].

There are many more U.S. and foreign public key management products for sale in the world, most of which support distributed key generation.

DATA SHEET III-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.
Technical Issues	Anonymity in commercial cybercash transactions on the Internet is a desirable feature for e-cash payment systems. However, anonymity introduces the potential for money laundering and counterfeiting. The Federal Reserve could have difficulty maintaining control of the money supply. The widespread use of e-cash would increase the vulnerability of national financial systems to INFOWAR attacks.
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 military supply decentralization and savings possible. Anonymous cash could be used in clandestine operations and certain special access programs (see Chairman, Joint Chief of Staff's *Joint Vision 2010*, the U.S. Army's FM 100-6, *Information Operations*, and the U.S. Air Force's *New World Vistas: Air and Space Power for the 21st Century*).

Some e-cash transfer systems are now in use and will be used more in the future by governments and in secure C4IFTW systems to provide cash disbursements for operations with widely dispersed forces. Integration of e-cash functionality into legacy military systems will be required. E-cash technologies are available in the United States; however, patents may encumber these technologies.

WORLDWIDE TECHNOLOGY ASSESSMENT

Australia	●	Canada	●●●●	France	●●●●	Germany	●●
Ireland	●	Israel	●	Netherlands	●●	New Zealand	●
Sweden	●	Switzerland	●	UK	●●●●	United States	●●●●

Legend: Extensive R&D ●●●● Significant R&D ●●● Moderate R&D ●● Limited R&D ●

The commercial sector is clearly leading the development of this technology. Many elements of e-cash systems are the product of years of basic research. Some producers of various types of e-cash systems, including e-cash and smart cards are:

- Canada: SCI™
- Finland: Avant
- France: Schlumberger and Bull
- Japan: Fujitsu, Hitachi, and NEC
- Netherlands: DigiCash™
- United Kingdom: Serif PLC and Mondex
- United States: Cyber-Cash™, CertCo., Bell South, Diebold, and Mastercard.

DATA SHEET III-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 to 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.
Technical Issues	Faith in the security of elliptic curve cryptographic systems is limited. Many argue that a longer period of peer review is necessary to establish the strength of elliptic curves and win the trust of potential users. Elliptic curve cryptography (ECC) offers high-efficiency and low overhead for encryption, digital signature, and key management applications because of its presumed strength (with shorter keys and high processor efficiency). This dual-use cryptographic technology is maturing rapidly. Additional R&D is required to prove, or firmly establish a universal belief in, the strength of elliptic curve cryptographic functions. International peer review, aided by the prizes offered by Certicom, will be a valuable supplement to funded R&D. There will be the usual requirement to integrate the commercial elliptic curve cryptographic functions with the other functionality in military applications.
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.

RATIONALE

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 2 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.

ECC is ideally suited to small, light C4IFTW portable field equipment. Elliptic curve systems may be particularly beneficial to RF device applications where processor power, bandwidth, and IC space may be limited. They may also be ideally suited to smart card and PC card applications that could be used to supply encryption and digital signatures to secure the transmission of orders and reports.

Several cryptographic suppliers will soon provide comparatively inexpensive tool kits for adding elliptic curve cryptographic functionality at standard cryptographic application programming interfaces (CAPIs) in military systems. Elliptic curves may soon be incorporated in the digital signature standard (FIPS Pub 186). 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.

WORLDWIDE TECHNOLOGY ASSESSMENT

Australia	●	Sweden	●●	Switzerland	●●	UK	●●●●
United States	●●●●						

Legend:	Extensive R&D	●●●●	Significant R&D	●●●	Moderate R&D	●●	Limited R&D	●

The civilian sector is driving the technical development of this technology. American National Standards Institute (ANSI) X9.F.1 is developing a standard for the use of elliptic curve systems by financial services in key management. Among the cryptography houses known to be developing elliptic curve systems are RSA [Security Dynamics] in the United States and Certicom in Canada.

RSA has announced an elliptic curve tool kit addition to their product line. Certicom is a center of expertise and probably the present industry leader. Eventually, most prominent cryptographic developers in the United States and overseas may offer cryptographic products based on elliptic curves.

DATA SHEET III-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.
Technical Issues	Present RBG methods that may be perform well in laboratories cannot yet be duplicated in versions that are suited to use in small, lightweight, inexpensive computers or data-capture peripherals. RBGs are available in the United States but may be encumbered by intellectual property rights. What seems to be needed is a ubiquitous RF (or similar) natural source that could inexpensively supply perfectly random bit streams, which could be supplied through a system somewhat similar to the way GPS provides location data.
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.

RATIONALE

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.

Small, portable C4IFTW terminals that have to generate keys on the battlefield will need optimized hardware random number generators (see Chairman, Joint Chief of Staff's *Joint Vision 2010*, the U.S. Army's FM 100-6, *Information Operations*, and the U.S. Air Force's *New World Vistas: Air and Space Power for the 21st Century*). Improved random bit strings could increase the strength of military encryption. To meet the requirements of trusted systems, hardware-based RBGs in commercial products must pass the FIPS Pub 140-1 randomness tests.

WORLDWIDE TECHNOLOGY ASSESSMENT

Australia	●●	Canada	●●●	France	●	Germany	●
Israel	●●●	Italy	●	Japan	●	Netherlands	●
New Zealand	●	Russia	●	Sweden	●●	Switzerland	●●
UK	●●	United States	●●●●				

Legend: Extensive R&D ●●●● Significant R&D ●●● Moderate R&D ●● Limited R&D ●

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; however, producers of COTS products that incorporate hardware-based random number generators were not identified.

DATA SHEET III-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.
Technical Issues	WANs often suffer from transitory disruption. This requires real-time data and key resynchronization. A key management infrastructure for key management must be put in place. Solutions and supporting standards for these high-speed network encryption problems and issues must be found soon.
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. (Cylink already has 45 Mbit/sec ATM encryption technology on the market.) 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.

RATIONALE

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, WANs. C4IFTW systems will increasingly depend on the global, installed telecommunications base of backbone "packet systems," which are rapidly replacing the legacy "circuit systems" (see Chairman, Joint Chief of Staff's *Joint Vision 2010*, the U.S. Army's FM 100-6, *Information Operations*, and the U.S. Air Force's *New World Vistas: Air and Space Power for the 21st Century*).

Leading edge HSE technologies will improve the overall speed and security of Global Command and Control Systems (GCCS) and C4IFTW systems. However, although commercial products will have to comply with applicable national and international standards to be marketable, they may not fully comply with the government security requirements. Military HSE technology products may require further development and integration. The United States has access to this technology through the USG-sponsored Fastlane and Key-Agile programs.

WORLDWIDE TECHNOLOGY ASSESSMENT

Australia	●●	Canada	●●●	France	●●	Germany	●●
India	●	Ireland	●	Israel	●●●	Italy	●●
Japan	●	Netherlands	●	New Zealand	●	Russia	●
South Africa Rep.	●	Sweden	●●●	Switzerland	●●●	UK	●●●
United States	●●●						

Legend: Extensive R&D ●●●● Significant R&D ●●● Moderate R&D ●● Limited R&D ●

The centers of HSE development are commercial. Fastlane is a USG-sponsored (622 Mbit/sec) ATM link encryption technology program. Key-Agile is another USG-sponsored encryption program that is developing the technology for encrypting each 53-byte cell in an ATM stream with a different key. Cylink sells InfoGuard 100™, a 45 Mbit/sec ATM encryptor; SECANT Network Technologies, Inc. has gained approval for exporting its 168-bit key DES CellCase™ ATM network security products; GTE, under contract with the USG for Fastlane, is considering a commercial ATM HSE version; and Microelectronics Center, under contract with the USG for Key-Agile (622 Mbit/sec), should be able to develop commercial HSE products. At least two U.S. firms are now marketing 45 Mbit/sec ATM encryption products. Interoperability, authentication, and access control features will require new protocols, which current high-speed, network-signaling protocols do not provide.

DATA SHEET III-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- to 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 to 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.
Technical Issues	Image steganography can be used to conceal an encrypted message. The technique of combining image steganography and encryption or multiple encryption could present an almost insoluble problem to National Security and law enforcement agency cryptanalysts. Even if a message were known to exist in an electronic image, the message bits would have to be identified and isolated for cryptanalysis. This process could make plaintext recovery time consuming—if not impossible. Some steganographic applications in the public domain could be made suitable for military use to supplement cryptography in their present COTS versions. In military applications, integration of the image steganographic functions and other functionality is required.
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.

RATIONALE

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.

Image steganography may be available through the LANL researchers, who hold the patent on a new method of image steganography. Widely available steganographic programs can incorporate a 64-kilobyte message in a 1024 × 1024 grayscale picture without changing the graphical image noticeably. The new LANL 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 protect military maps and other sensitive defense imagery by making it possible to detect spoofing attempts that might have been made during transmission. It could be used to guarantee the integrity of picture badges and identification cards. It would also be useful in maintaining the security of sensitive operations, covert operations, and special access programs.

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.

WORLDWIDE TECHNOLOGY ASSESSMENT

Australia	●●	Belgium	●	Canada	●●●	South Africa Rep.	●
Sweden	●●●	Switzerland	●●●	UK	●●●●	United States	●●●●

Legend: Extensive R&D ●●●● Significant R&D ●●● Moderate R&D ●● Limited R&D ●

The apparent USG center of image steganography R&D is LANL. There are developers like SynData Technologies, Inc. in the United States and Deus Ex Machina Communications in Germany that may be conducting proprietary image steganography R&D. Also, Colon Moroney, the U.S. author of *Hide and Seek for Win95*, is a candidate developer.

A total of 31 programs have been written for 6 different operating systems available on the Internet for embedding messages in graphics. U.S. companies sell six of the seven Windows programs. One Windows program, *Steganos for Win95*, is produced in Frankfurt, Germany. Source code for 10 of these steganographic products is also available.

DATA SHEET III-10.4. KEY MANAGEMENT

Developing Critical Technology Parameter	The *Infosecurity News Buyers Guide* for 1998 lists more than 27 data encryption key management products. Early versions of this technology are here now. However, it may be 10 to 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.
Technical Issues	A major key management issue in the use of asymmetric-key systems is the establishment of the pairs of secure keys. Using either symmetric-key or asymmetric-key techniques, the key management problem becomes a crucial issue, especially if the network is large. Although the USG has access to this technology, considerable R&D work will be required over the next 10 years to develop and maintain the level of trust required for military applications and infrastructure assurance. Integration of commercial key management functions with the other functionality in military applications is required.
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.

RATIONALE

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.

Both NIST and ANSI have published key management standards; however, because the NIST and ANSI standards were not developed for C4IFTW systems, DoD is developing a program that includes key management experiments and demonstrations. In some C4IFTW systems, large networks exist in which many possible two-party communications could take place. 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.

WORLDWIDE TECHNOLOGY ASSESSMENT

Argentina	●	Australia	●●●	Austria	●	Belgium	●
Canada	●●●●	South Africa Rep.	●	Sweden	●●	Switzerland	●●
UK	●●●●	United States	●●●●				

Legend: Extensive R&D ●●●● Significant R&D ●●● Moderate R&D ●● Limited R&D ●

The USG is leading an effort to establish an FPKI. NIST has an FPKI Working Group that includes many members from the financial banking services and industries that produce key management products or offer Certification Authority services. The USG is also receiving key management support from industry. The Navy is developing a program to distribute and manage cryptographic keys for all the military Services and some USG civilian services. SAIC has a 3-year Navy contract to distribute and manage cryptographic keys for all of the military Services and some USG civilian agencies.

Industry and standards organizations are leading the development of public key infrastructures for e-commerce. The top five key management companies are Certco, IBM, Cyber Trust [GTE], and VeriSign in the United States and Entrust in Canada. Other prominent U.S. key management system developers, producers, and service providers are AT&T, Atalla, Cylink, Lockheed Martin, Prime Factors, RSA Data Security, Inc. [Security Dynamics], SAIC, and ViaCrypt [Network Associates]. Many others provide key management products and services. There are also companies developing these products and services in Europe and Asia.

DATA SHEET III-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.
Technical Issues	The commercial key recovery technology is maturing rapidly. A general key escrow system is equivalent to (can be reduced to) a chosen-ciphertext-secure system, and an escrow system (with certain accountability features) is equivalent to a non-malleable cryptosystem. Much is known about chosen-ciphertext-secure and non-malleable cryptographic systems. Integration of the commercial key recovery functions with the other functionality in military some applications is required. Patents encumber these technologies. Basic research in protocols is required for early discovery of any flaws that might be inherent in these systems.
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.

RATIONALE

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.

An improved theoretical underpinning for escrow/recovery agent archiving systems might help to silence some of the opponents of the USG key escrow policy. KRSs are an important factor in military continuity of operations planning. In anticipation of the use of public key systems for key management in some military systems, key recovery systems and protocols will be required to provide emergency access to encrypted data. The European Community has formally rejected the U.S.-sponsored key escrow requirements.

WORLDWIDE TECHNOLOGY ASSESSMENT

Australia	●●	Canada	●●●	Sweden	●	Switzerland	●
UK	●●	United States	●●●●				

Legend: Extensive R&D ●●●● Significant R&D ●●● Moderate R&D ●● Limited R&D ●

There are shared Centers of Excellence in government and the private sector for key escrow/recovery technology development. Trusted Information Systems (TIS™) and IBM are probably the leading key recovery pioneers and may be the current leading producers of key recovery systems. However, the Key Recovery Alliance now has 71 international members. The long-term objective of the Key Recovery Alliance is the global deployment of interoperable, customer-driven key recovery.

Other developers are certain to challenge this leadership. There are already 33 products offering different key recovery schemes, with characteristics yielding different operational and security capabilities.

DATA SHEET III-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.
Technical Issues	The MCP/TOPS Whitney computer will have a new all-hardware operating system that will be incompatible with the installed base of legacy software operating systems. When the Whitney gets beyond the concept definition phase, the biggest issue will be the cost for the replacement of the installed base of legacy operating systems. Also, applications for the Whitney computer will have to be written, rewritten, or transliterated into versions that will run on the new TOPS operating system.
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 mainframe 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.

RATIONALE

This is a new information processing concept advocating a completely new computer architecture standard that could eventually replace the current von Newmann 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.) The APLS could provide a highly secure, high-speed processing system ideally suited to military information processing requirements (see Chairman, Joint Chief of Staff's *Joint Vision 2010*, the U.S. Army's FM 100-6, *Information Operations*, and the U.S. Air Force's *New World Vistas: Air and Space Power for the 21st Century*). 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. The United States has the only access to this technology at this time. The three joint patent holders are U.S. citizens, and the United States is the unilateral leader in this technology. Since the Whitney could significantly enhance U.S. competitiveness, this technology

should not be transferred to foreign business interests. A Whitney MCP/TOPS principal is Dr. Edward Davis of North Carolina State University, Computer Science, 226 Withers Hall, Raleigh, NC 27695.

WORLDWIDE TECHNOLOGY ASSESSMENT

United States	●

Legend: Extensive R&D ●●●● Significant R&D ●●● Moderate R&D ●● Limited R&D ●

The center of development for the MCP/TOPS Whitney computer is commercial at this time. The MCP/TOPS computer is still in the concept development phase and is not yet in production. The Whitney Computing Company of 54 Holly Lane, Darien, CT 06820 holds the MCP/TOPS patent and will be the developer and initial producer. No foreign competitor to the Whitney computer concept has been identified.

DATA SHEET III-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.
Technical Issues	The equivalence of digital signatures with written signatures is still in question. Most authorities believe that the electronic equivalent should be recognized as having the same legal status as a written signature. However, digital signatures have not yet been directly challenged in court. Since no large body of case law exists, some authorities still question their legal status. Key management security questions must still be answered. Investigations of the security of existing digital signature schemes should be continued..
Major Commercial Applications	The major commercial applications will be those developed for e-commerce.
Affordability	Not an issue.

RATIONALE

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.

Message integrity and non-repudiation authentication are important to the full cycle of military command and control from orders to situation reports (see Chairman, Joint Chief of Staff's *Joint Vision 2010*, the U.S. Army's FM 100-6, *Information Operations*, and the U.S. Air Force's *New World Vistas: Air and Space Power for the 21st Century*). Classified military information is protected by Type I USG cryptographic systems, which should provide message integrity and non-repudiation authentication. However, some sensitive, but unclassified, defense information and other USG information will require a guarantee of message integrity or non-repudiation authentication protection.

There is a requirement to integrate the commercial digital signature cryptographic functions with the other functionality in tailored military applications. COTS applications that DoD is likely to use to protect sensitive unclassified traffic have digital signature systems that could be easily integrated. There is a digital signature standard (FIPS Pub 186) for sensitive but unclassified USG text, files, and data.

WORLDWIDE TECHNOLOGY ASSESSMENT

Argentina	●●	Australia	●●●	Austria	●●●	Belgium	●●●
Canada	●●●	China	●●●●	Czech Republic	●●	Denmark	●●●
Finland	●●●	France	●●●●	Germany	●●●●	Greece	●
Hong Kong	●	India	●●	Iran	●	Ireland	●●●
United States	●●●●						

Legend: Extensive R&D ●●●● Significant R&D ●●● Moderate R&D ●● Limited R&D ●

The commercial sector and governments are driving the development of trusted message integrity and non-repudiation authentication systems for commercial and government applications. The United States is probably the leading producer of digital signature products. Many companies that have been listed as suppliers of products for data protection also produce products that perform message integrity and non-repudiation authentication functions. Examples are:

- Canada: Entrust
- United States: AT&T, Atalla, CKS, Cybersafe, Cygnus Solutions, Cylink, Enigma Logic, Spyrus, IBM, Lockheed Martin, Motorola, Netscape, Semantec, RSA [Security Dynamics], TIS [Network Associates], and Wang Government Services.

DATA SHEET III-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 to 10 years.
Critical Materials	None identified.
Unique Test, Production, Inspection Equipment	None identified.
Unique Software	None identified.
Technical Issues	This technology is not yet accredited and has not undergone an extensive field operational testing period. The associated operational and maintenance protocols must be developed and tested.
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.

RATIONALE

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.

This technology will make INFOSEC functionality more affordable for military forces and civilian organizations by reducing the cost of changing hosts and extending the useful life of the INFOSEC modules (see Chairman, Joint Chief of Staff's *Joint Vision 2010*, the U.S. Army's FM 100-6, *Information Operations*, and the U.S. Air Force's *New World Vistas: Air and Space Power for the 21st Century*). It could be used in C4IFTW systems and subsystems that incorporate cryptographic functionality. It has not yet been proven to be suitable for commercially viable products, and COTS products offering this technology may not be immediately available. Commercial programmable, embeddable COMSEC technology products have not been identified.

An example of this technology is the Programmable Embeddable INFOSEC Product (PEIP) being developed by the Naval Research Laboratory (NRL). PEIP emulates multiple cryptographic devices using cryptographic channels. Once configured, PEIP can encrypt, decrypt, and generate keystreams without intervention. Other embeddable COMSEC efforts are the Advanced INFOSEC Module and the Cornfield Embeddable COMSEC program.

No other development efforts were identified. For the foreseeable future, access to the programmable, embeddable COMSEC technology will have to be through the NRL contractors and subcontractors.

WORLDWIDE TECHNOLOGY ASSESSMENT

Australia	●●	Canada	●●	France	●	Germany	●
India	●	Ireland	●	Israel	●●	Italy	●
Japan	●	Netherlands	●	New Zealand	●	Russia	●
South Africa Rep.	●	Sweden	●●	Switzerland	●●	UK	●●●
United States	●●●						

Legend: Extensive R&D ●●●● Significant R&D ●●● Moderate R&D ●● Limited R&D ●

The NRL is the present government center of development. Motorola, Raytheon, Group Technologies, and Tracor are commercial centers of development. Since the programmable, embeddable COMSEC technology is in the prototype phase of development, there are no major producers at this time; however, there may be potential producers among the NRL contractors and subcontractors. Motorola is currently working on the Advanced INFOSEC Module and Raytheon Corporation is working on the Cornfield Embeddable COMSEC program.

DATA SHEET III-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.
Technical Issues	A fundamental rule for generating keys requires that every bit of the active key be generated or selected at random such that every possible combination of bits in a key has an equal probability of being selected. A cryptographically secure random number generator must not only generate statistically random sequences, but it must be computationally infeasible to predict what the next random bit will be, given complete knowledge of the algorithm or hardware generating the sequence and all of the previous bits in the stream. Pseudo-random bit generation is one of the fertile areas of cryptology research.
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.

RATIONALE

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. These keys must be unknown to an adversary, and software random number generators are the best-known method for producing such keys. High-security military plans and operations must be protected by secure cryptography. Perfect randomness, the equivalent of the old signal one-time pads, is required for strong cryptographic systems (see Chairman, Joint Chief of Staff's *Joint Vision 2010*, the U.S. Army's FM 100-6, *Information Operations*, and the U.S. Air Force's *New World Vistas: Air and Space Power for the 21st Century*).

Many forms of cryptography used in C4IFTW ISs 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.

WORLDWIDE TECHNOLOGY ASSESSMENT

Australia	●●	Austria	●	Belgium	●	Canada	●●●●
Denmark	●	Finland	●	France	●●●	Germany	●●●
India	●	Ireland	●●	Israel	●●●●	Italy	●●
Japan	●●	Netherlands	●●●●	New Zealand	●●	Russia	●●●●
South Africa Rep.	●●	Sweden	●●●●	Switzerland	●●●●	UK	●●●●
United States	●●●●						

Legend: Extensive R&D ●●●● Significant R&D ●●● Moderate R&D ●● Limited R&D ●

Both government and industry conduct secret and proprietary random number generation R&D and maintain centers of development for this technology. U.S. manufacturers who comply with ANSI X9 (Financial Services) incorporate random number generators in their cryptographic modules. Underdeveloped producers also offer products that have PRBGs.

DATA SHEET III-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. NIST Researchers in Boulder, Colorado, have already built and tested a simplified version; however, 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.
Technical Issues	If there is less than perfect isolation, decoherence error could become an overwhelming problem affecting the accuracy of quantum computers. Decoherence is caused by continuous interaction between the system (in this case, the quantum computer) and the environment. Ultimately, the survival of the promise of general-purpose quantum computing lies in the success of quantum error correction. Specific product development programs may be proprietary. The quantum computer could be regarded as a hybrid R&D challenge because both hardware and significant software work will be required.
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.

RATIONALE

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 military and civilian 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 Newmann 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) that could be of military value and importance. 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.

WORLDWIDE TECHNOLOGY ASSESSMENT

United States ●

Legend: Extensive R&D ●●●● Significant R&D ●●● Moderate R&D ●● Limited R&D ●

The United States has the unilateral lead in quantum computer technology. There is considerable commercial and academic interest in quantum computers; however, there are no producers or developers at this time. This technology is still in the research stage.

NIST is the center of USG R&D. IBM and AT&T are probably the leading commercial centers of research. Active scientists include Don Simon of Microsoft Corporation in Redmond, Washington; Ignacio Cirac of the University of Castilla-La Mancha in Spain; Peter Zoller of the University of Innsbruck in Austria; Richard Hughes of LANL; David DIVincenzo and Charles Bennett of IBM's Thomas J. Watson Research Center in Yorktown Heights, New York; and P.W. Shore, AT&T Bell Laboratories of Murray Hill, New Jersey.

DATA SHEET III-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.
Technical Issues	The present limitation is range since any amplification technology (even laser-pumped, erbium-doped fiber) changes the photon's quantum characteristics. Quantum-encrypted signals have been successfully transmitted over ordinary optical fiber only 48 km (~ 30 miles).
Major Commercial Applications	No immediate commercial applications for quantum encryption were identified.
Affordability	Not an issue.

RATIONALE

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. No reports of quantum encryption technology work outside the United States have been identified. The only experiments being carried out are at LANL.

This technology could be used to transmit ultra-sensitive military information and objects, such as secret encryption algorithms or master keys (see Chairman, Joint Chief of Staff's *Joint Vision 2010*, the U.S. Army's FM 100-6, *Information Operations*, and the U.S. Air Force's *New World Vistas: Air and Space Power for the 21st Century*). It could also be used to send sensitive messages, secret encryption algorithms, or master keys between C4IFTW nodes. Even with the present range limitation, quantum encryption could be used between command centers clustered relatively close together (e.g., in the Washington Metropolitan Area and on Oahu, Hawaii). If some discovery eliminates the present range limitation, this technology could be used between all C4IFTW nodes served with fiber-optic connectivity.

WORLDWIDE TECHNOLOGY ASSESSMENT

Argentina ● United States ●

Legend: Extensive R&D ●●●● Significant R&D ●●● Moderate R&D ●● Limited R&D ●

The only identified center of quantum encryption development is the LANL. No commercial developers or producers of quantum encryption systems were identified. The only R&D work, outside academia, is either classified or proprietary experimental laboratory work, and reports have not been located in open source material.

DATA SHEET III-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. A simple example of a military secret sharing scheme is the one used for the two-man control of nuclear weapons. The execution order verification code is divided between two crew members so that both crew members must contribute their part of the code to verify that an order is valid and authentic. Various forms of this technology are application ready now; however, mathematically provable schemes may be 5 to 10 years away.
Critical Materials	None identified.
Unique Test, Production, Inspection Equipment	None identified.
Unique Software	None identified.
Technical Issues	The proactive signature schemes ensure that the private key is never assembled in one place where it could be compromised and are more sophisticated versions of secret sharing. (The proactive signature techniques are important in Root or Bridge Certification Authority applications.) There may be intellectual property issues.
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.

RATIONALE

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.

Improved secret sharing schemes are needed to increase the robustness, reliability, and availability of key management in C4IFTW systems. Secret sharing schemes would be useful for split control keys for functions such as nuclear multi-party control and for key availability. As an example, the key could be split into 10 pieces, any 7 of which could be used to reconstitute the key (see Chairman, Joint Chief of Staff's *Joint Vision 2010*, the U.S. Army's FM 100-6, *Information Operations*, and the U.S. Air Force's *New World Vistas: Air and Space Power for the 21st Century*).

Secret sharing schemes could serve as an authentication scheme for orders and reports in sensitive operations. These schemes have applications in C4IFTW systems to provide secure methods for the channels of communications from the NCA to the weapon system commanders. Primitive forms are in use now for authenticating nuclear control orders in the C2 systems for nuclear weapons. 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.

WORLDWIDE TECHNOLOGY ASSESSMENT

Australia	●●	Canada	●●●●	France	●●	Germany	●●
Israel	●●	Netherlands	●	Russia	●●	Sweden	●●
Switzerland	●●	UK	●●	United States	●●		

Legend: Extensive R&D ●●●● Significant R&D ●●● Moderate R&D ●● Limited R&D ●

The USG developed the basic secret sharing scheme for nuclear control orders. Commercial interests have large secret sharing R&D efforts. Commercial interests want schemes that can be used in commercial key recovery systems and key management infrastructures. A provision for secret sharing to protect master and private keys is incorporated in the key management systems developed and produced by AT&T, Atalla, CertCo, Cylink, IBM, Lockheed Martin, Prime Factors, and RSA Data Security, Inc. [Security Dynamics] in the United States and Entrust in Canada. This is not a complete list of producers. This list was arbitrarily compiled from a 1998 list of key management system developers.

DATA SHEET III-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.
Technical Issues	There are many published stream ciphers. Most have been developed for simplicity and ease of implementation. A stream cipher applies simple encryption transformations, according to the keystream being used. There are still discoveries to be made in the generation of optimum keystream ciphers, and research is needed to develop optimum encryption transformations for the type of keystream being used. Developmental integration effort will be required in this technology for use with or in weapons systems. Most stream ciphers that are incorporated in cryptologic applications are either proprietary or highly classified. Governments universally classify the cryptologic applications developed for military and government use in protecting classified information. Some of the COTS applications that could be put to military use may contain stream ciphers.
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.

RATIONALE

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. Stream ciphers are a form of cryptography that is well suited to the protection of military RF links with small, lightweight C4IFTW portable field equipment. They are also 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.

WORLDWIDE TECHNOLOGY ASSESSMENT

Argentina	●	Australia	●●●●	Austria	●●	Belgium	●●●●
Canada	●●●●	China	●	Costa Rica	●●●	Czech Republic	●●
Denmark	●●●●	Finland	●●●	France	●●●●	Germany	●●●●
India	●●●	Iran	●●	South Africa Rep.	●●	South Korea	●●
Sweden	●●●●	Switzerland	●●●●	UK	●●●●	United States	●●●●

Legend: Extensive R&D ●●●● Significant R&D ●●● Moderate R&D ●● Limited R&D ●

Governments may be the center of stream cipher development. Since any government-sponsored stream cipher R&D in progress would be classified, the status of such programs cannot be independently assessed. Similarly, commercial developments are proprietary. Therefore, the center of stream cipher development has not been identified. Informal information indicates that the following are U.S. stream cipher developers and producers: RSA Data Security, Inc. [Security Dynamics], IBM, Cylink, and Motorola. There may be companies developing products in Europe and Asia that have not announced or prominently advertised their stream cipher products.

DATA SHEET III-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. There is a continuing C4IFTW requirement for authentication and verification of execution orders and situation reports, certain categories of which might benefit from the incorporation of ZNP schemes.
Critical Materials	None identified.
Unique Test, Production, Inspection Equipment	None identified.
Unique Software	None identified.
Technical Issues	ZNP protocols are difficult to implement and can be computationally intensive and time consuming. ZNP systems are available in the United States but may be encumbered by intellectual property rights. Although there has been extensive basic and applied scientific research has been coordinated on minimum-disclosure and various types of ZNP, this is still an open field of research.
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.

RATIONALE

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.

There may be unique defense requirements for ZNP systems. Some form of ZNP might be adapted for use in IFF systems, which could be used to reduce the incidence of inadvertent engagements in combat (see Chairman, Joint Chief of Staff's *Joint Vision 2010*, the U.S. Army's FM 100-6, *Information Operations*, and the U.S. Air Force's *New World Vistas: Air and Space Power for the 21st Century*). Efficient ZNPs must be tailored to and integrated into each application.

WORLDWIDE TECHNOLOGY ASSESSMENT

Australia	●●	Canada	●●●	France	●	Germany	●
India	●	Ireland	●	Israel	●●●	Italy	●
Japan	●	Netherlands	●●●	New Zealand	●●	Russia	●●●
South Africa Rep.	●	Sweden	●●●	Switzerland	●●●	UK	●●●●
United States	●●●●						

Legend: Extensive R&D ●●●● Significant R&D ●●● Moderate R&D ●● Limited R&D ●

There are commercial ZNP R&D efforts to produce schemes that are suitable for use in various forms of e-commerce. In the United States, this is an area of intensive research by DigiCash and CertCo, but no commercial products were identified.

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, IO, and ISs and the ISs configured to provide capability to manage and control entities, systems, devices, processes, organization, and events whose primary purpose and application are other than IOs or ISs.

Historically, most advanced IM&C technology and standard 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 and 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 LANs comprising 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" IM&C. 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:

1. The International Standards Organization (ISO) has been working on several 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.

2. 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).

3. 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).[14]

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

---

14 LLC stands for Logical Link Control.

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.[15]

ISO/Internet management frameworks are based on the Agent Process/Manager Process paradigm, depicted conceptually in Figure 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.

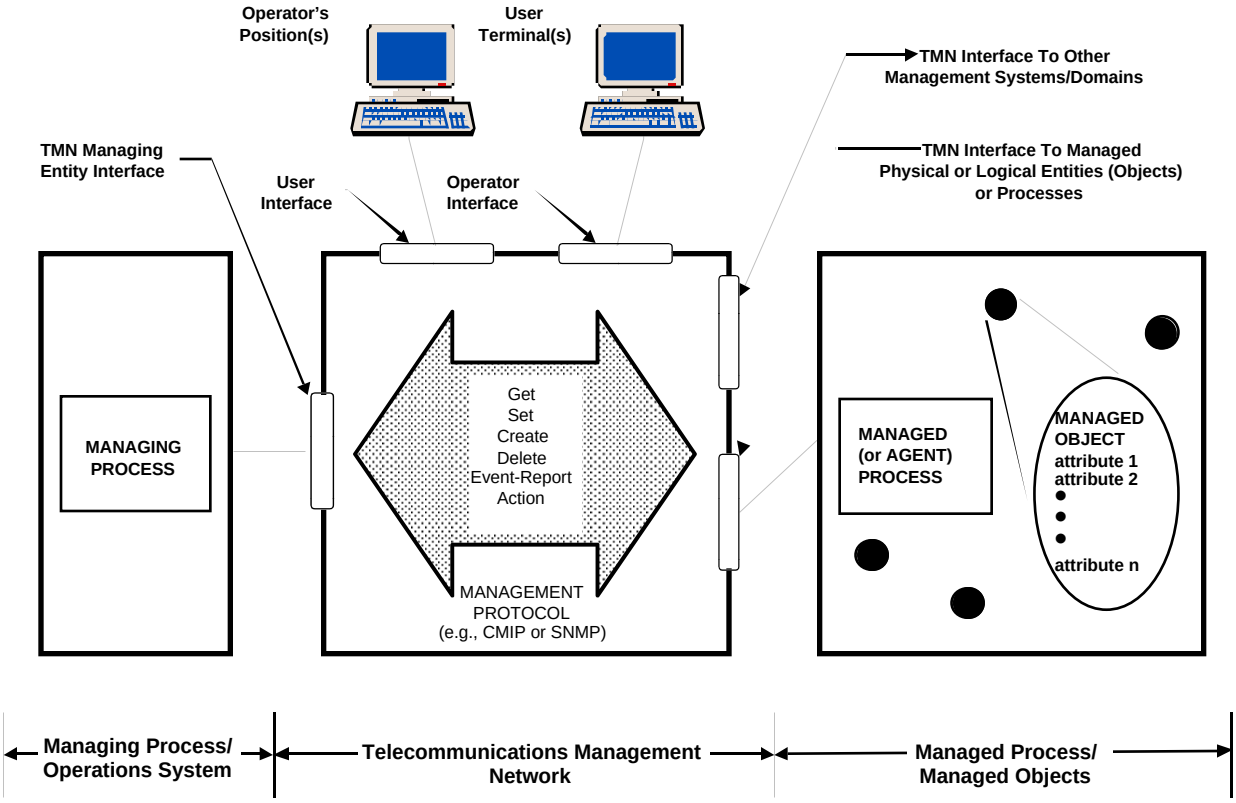


Figure 10.5-1. Agent Process/Manager Process Paradigm

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

15 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).

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.

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 Figure 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 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.

Figure 10.5-2 summarizes IM&C capabilities (i.e., the cardinal IM&C functions, IM&C domain categories, and categories of managed and controlled entities, objects, and events) described in the preceding discussion. Considering the breadth of possible applications, it is not surprising that users, product vendors, and standards-setting groups classify and organize IM&C functions differently. The functional decomposition depicted in the figure uses five canonical or largely non-overlapping subareas, under which functions specified in ISO/OSI, Internet, IEEE, and other standards-setting organizations—as well as functions defined in proprietary vendor products—can be accommodated. Of course, the managed and controlled entities/events items listed represent only examples of a very large set of possibilities.

RATIONALE

Without effective NM and control, complex voice, data, video, or integrated telecommunications, networks are simply not possible. In the past, truly effective communications NM was primarily the domain of the old Bell System and the PTTs. More recently, new carriers and most private network operators—left with inadequate NM by divestiture and privatization—have discovered its central importance.

From a business perspective (or from a government, military, or private network operational cost perspective), many operators have concluded that network administration and billing (or cost allocation) systems are as critical as

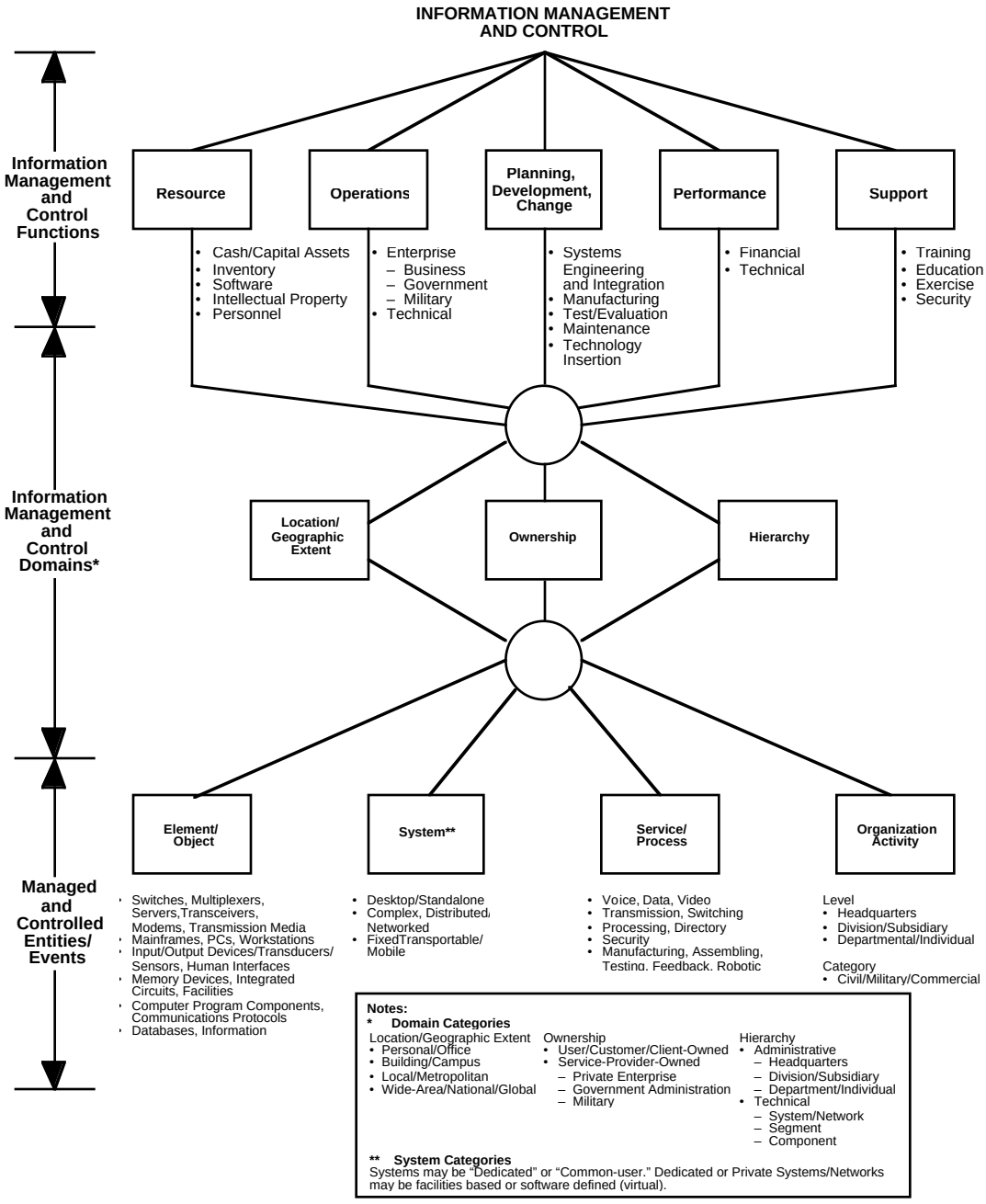


Figure 10.5-2. IM&C Capabilities

switching and transmission. For example, the underlying cost for a hypothetical fiber-optic, full-duplex link between New York and Los Angeles is currently projected at about 2.6×10^{-8} cents per bit or about 18/100ths of a cent for a 1-minute conversation. At these prices, administrative costs exceed transmission costs by an order of magnitude.

In the last several years, we have witnessed significant progress in reducing administrative costs. For example, one of the nation's largest telephone companies announced a 13-percent reduction in its workforce (17,000 jobs). This company stated that automation and more efficient computerized equipment allowed it to reduce the number of network management centers from 19 to 1 and to consolidate 171 customer service centers into just 11 locations.

Overall, the number of employees per 10,000 lines is expected to drop from 42 to the low 30s, a productivity improvement of 20 percent.

NM is as critical to achieving reliability, availability, and continuity of service goals as it is to cost-effective operations. Historically, in public switched voice networks (PSVNs), communications NM is synonymous with mechanisms that prevent catastrophic loss of service caused by congestion resulting from heavy traffic overloads or network element failure.

Normally, transmission networks and common-control switching systems make efficient use of facilities by distributing traffic among alternate paths as the primary routes reach capacity. However, in the absence of modern IM&C and signaling systems, when traffic loads exceed engineered levels (e.g., Three Mile Island and the Los Angels earthquake or when failures occur), continued call attempts may actually decrease usable capacity and the number of calls that a network can carry. Unchecked, such situations result in a degenerative process that quickly leads to widespread service disruption throughout an entire network.

In the past, NM and control system limitations have placed responsibility for continuity of service during crisis situations squarely in the hands of experienced and knowledgeable human network administrators. Today's advanced digital switching and fiber-optic transmission systems offer significantly more capacity than the capacity offered just a few years ago. However, because these systems tend to concentrate ever-increasing amounts of traffic within single switching and transmission mechanisms (the "funnel factor") to avoid extended and large-scale service interruptions, these new technologies mean higher levels of pre-planned routing diversity and improved, computer-assisted, automated, and near-real-time management systems. The fire in Hinsdale, Illinois, the blackout in Manhattan, and the recent loss of one vendor's Internet service are examples of catastrophic failures that produce prolonged service interruptions—situations that must and can be avoided in the future.

To offset the greater risk associated with failures, enhanced survivability and security are key attributes and objectives in SDH specifications for emerging SONET and International Telecommunications Union-Telecommunications Standard (ITU-TS) transmission systems. SDH/SONET-based BLSRs provide reusable bandwidth for more efficient internode transport in evenly meshed networks and greatly increase reliability and survivability. 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 switching and routing.

In conjunction with ITU TMN-based management functions (or vendor product equivalents), this can result in unparalleled recovery from transmission failures—whether these failures occur naturally or from intended or collateral enemy attack damage. Recent progress in automatic restoration of broadband systems is dramatic. For example, in November 1988, a backhoe severed a primary Washington-to-New York fiber cable, disrupting service for 16 hours. In August 1992, a similar mishap in Mississippi disconnected tens of thousands of circuits, all of which were restored within 5 minutes. This improvement was made possible by computer-based, rapid-acting, automated restoration, and real-time network routing IM&C systems.

Although military systems can be built to exhibit higher levels of resistance to certain types of threats (e.g., nuclear radiation and HEMP) and excess capacity can be designed into military systems to account for losses in warfare, capacity requirements sufficient to handle peacetime civilian traffic are generally orders of magnitude larger than any justifiable military overbuild design. Consequently, IM&C technologies enabling public telecommunications to be restored and/or reconfigured rapidly for military purposes during conflict situations are clearly the most effective strategies against large-scale physical attacks. While the greatest advancement in automated complex IM&C has occurred in the commercial sector, IM&C is a prime example of a function that enables clever adversaries to use commercial technology as an effective weapon in their war-making arsenals (as discussed in more detail in MCTL, Part II, Section 2).

Beyond military criticality issues, national economic security is enhanced when superior IM&C leverages the U.S. share of the multi-trillion dollar worldwide IT market. Even though much IM&C development occurs as an adjunct to telecommunications, those capabilities, because of the confluence of computers and communications, find widespread use in most IT applications and in many non-IT markets in which ITs are key to business operations.

For example, the PC hardware and computer software industries have adapted, improved, and now almost totally rely upon automated, real-time customer service centers pioneered in mobile communications and LAN and WAN administrative "help desk" installations. Shipping and transportation industries employ sophisticated package tracking and inventory/conveyance control programs upon which efficient operations and competitive market positions are critically dependent. Moreover, in designing and developing such complex systems, computer-based systems engineering and integration support are now an indispensable project management tools. Automatic process control in manufacturing and in testing during manufacturing are similarly crucial for successful, low-cost, high-quality production. Executive, mid-level, and departmental organization, planning, and problem-solving operations are becoming increasingly dependent upon modern, local, and distributed (teleconferencing) hardware, software, and network-based "decision-support" management capabilities—whether these resources are used for commercial, civilian, or military enterprises.

A final example of economic and military rationale for IM&C criticality is the need for industrial training and education. Streamlining planning, development, and production has produced crises in sectors where it is possible to introduce new high-technology products and equipment (weapons for military situations) faster than company or military personnel can be trained to market, support, or employ them. Responding to this need, personnel managers are applying a growing inventory of advanced, hypermedia-based classroom, distance-learning, and self-study technologies. This trend is shifting the balance from predominately classroom and other off-premises arrangements to on-job training—an action that, implemented properly, saves time and money while improving learning. Today's successful education and training approaches do not merely employ new hardware and software technologies to existing learning processes; rather, breakthroughs occur only when managers employ new pedagogies that optimize learning through advanced IT capabilities. In this regard, as in CMIP/SNMP management standards, new paradigms, new implementing architectures, and even a new "structure of training information" (i.e., the arrangement and presentation of scientific and technical information) need to be defined.

Complementing education and training trends are expanding abilities for remote "technology insertion." As a generally accepted practice, software upgrades are downloaded via networks with minimal or no user or local operator participation. Standards-based "plug and play" hardware and automatic "managed object" reporting and location further support and dramatically enhance traditional configuration management and change control.

Figure 10.5-2 indicates that effective planning, development, implementation, operation, and maintenance of all ITs are critically dependent upon IM&C capabilities. Although many ITs are rapidly achieving commodity status and can easily be acquired in world markets, their assembly into useful and sustainable industrial or military operating entities is totally dependent upon IM&C systems and the knowledgeable and competent individuals who create them.

WORLDWIDE TECHNOLOGY ASSESSMENT (see Figure 10.5-3)

Figure 10.5-3 contains the IM&C Technology WTA summary. Most of the IM&C R&D is being done by commercial organizations in Canada, Germany, Israel, Sweden, the United Kingdom, and the United States. Other countries construct individualized software systems using commercially available software for network control, system monitoring, and protection.

Country	Resources	Operations	Planning Development Change	Performance	Support
Australia	●●●●	●●●●	●●●●	●●●●	●●●
Austria	●●●	●●●	●●●	●●●	●●●
Belgium	●●●	●●●	●●●	●●●	●●●
Canada	●●●●	●●●●	●●●●	●●●●	●●●●
China	●●●	●●●	●●●	●●●	●●●
Costa Rica	●●	●●	●●	●●	●●
Cuba	●●	●●	●●	●●	●●
Czech Republic	●●	●●	●●	●●	●●
Denmark	●●●●	●●●●	●●●●	●●●●	●●●●
Egypt	●●	●●	●●	●●	●●
Finland	●●●●	●●●●	●●●●	●●●●	●●●●
France	●●●●	●●●●	●●●●	●●●●	●●●●
Germany	●●●●	●●●●	●●●●	●●●●	●●●●
Hungary	●	●	●	●	●
India	●●●	●●●	●●●	●●●	●●●
Iran	●	●	●	●	●
Iraq	●	●	●	●	●
Ireland	●●●	●●●	●●●	●●●	●●●
Israel	●●●●	●●●●	●●●●	●●●●	●●●●
Italy	●●●	●●●	●●●	●●●	●●●
Japan	●●●●	●●●●	●●●●	●●●●	●●●●
Libya	●	●	●	●	●
Netherlands	●●●●	●●●●	●●●●	●●●●	●●●●
New Zealand	●●●	●●●	●●●	●●●	●●●
North Korea	●	●	●	●	●
Norway	●●●●	●●●●	●●●●	●●●●	●●●●
Pakistan	●●	●●	●●	●●	●●
Poland	●●●	●●●	●●●	●●●	●●●
Russia	●●	●●	●●	●●	●●
South Africa	●	●	●	●	●
South Korea	●●	●●	●●	●●	●●
Sweden	●●●●	●●●●	●●●●	●●●●	●●●●
Switzerland	●●●	●●●	●●●	●●●	●●●
Syria	●●	●●	●●	●●	●●
Taiwan - R.O.C.	●●●	●●●	●●●	●●●	●●●
UK	●●●●	●●●●	●●●●	●●●●	●●●●
United States	●●●●	●●●●	●●●●	●●●●	●●●●

Legend: Extensive R&D ●●●● Significant R&D ●●● Moderate R&D ●● Limited R&D ●

Figure 10.5-3. IM&C Technology WTA Summary

LIST OF TECHNOLOGY DATASHEETS
III-10.5. INFORMATION MANAGEMENT AND CONTROL

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 III-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.
Technical Issues	Transaction sequencing.
Major Commercial Applications	Internet usage by general public.
Affordability	Cost will be less than current solutions.

RATIONALE

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.

For the military, this has tremendous implications. With the adoption of wearable computers, each warfighter could have access to information and processing power with the individualized security that comes with applications such as voice recognition—but without interfering with necessary physical functions. This individual would also have much broader access to information, command, and personal communications than that which is currently available.

Commercial development will go a long way as the basis for such systems, but the military user will have additional special needs, particularly for security, fast access, and, in some cases, consolidation of data with associated analysis.

WORLDWIDE TECHNOLOGY ASSESSMENT

Australia	●●	France	●●●	Germany	●●●●	Japan	●●●●
Sweden	●●●●	UK	●●●●	United States	●●●●		

Legend: Extensive R&D ●●●● Significant R&D ●●● Moderate R&D ●● Limited R&D ●

Any country with a big presence in the current telecommunications marketplace must have extensive R&D in this area. Mobile phones, hand-held computer input devices, and even stationary phones are beginning to use this technology. Also, several of the more popular Internet sites are providing capability in their servers that previously had been accomplished on individual PCs or individual computers. Examples of server-provided software and data storage can be found in some of the Internet stock-tracking sites. Such a site would identify a particular user, accept input on stocks of interest to the user, access stock trading databases available to the server, and provide the user with spreadsheets, graphs, news, and so forth based upon the user request.

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 IS Facilities FA is defined as capabilities to house, energize, transport, protect, and provide appropriate operating conditions and/or human habitation and life support for IS infrastructures under benign, naturally occurring, manmade, conventional, chemical, biological, or nuclear warfare environments.

IS facilities encompass any or all of the following capabilities: exterior physical shelter and interior room; equipment and other IS support structures; prime power generation and/or co-generation; power conditioning; environmental heating, ventilation, and air-conditioning (HVAC); chemical and biological filtration and protection; EMP protection; TEMPEST shielding; radiation protection; and human habitation and life-support accommodations. IS facilities are used to collect, monitor, and protect information in a variety of ways appropriate to a particular mission or operational condition. Facilities can be attended or unattended by humans. They may be either physically occupied or remotely attended. Facilities can be designed for either defensive and/or offensive purposes. Some facilities may be intended for human occupation, occasionally occupied, or never intended for human visitation. Thus, facilities will need to be designed with a capacity for automated self-protection, automated maintenance and repair, and automated disaster detection and recovery—all of which must be performed in a reliable, secure manner. Figure 10.6-1 is a taxonomy of major IS facilities capabilities.

Clearly, not all these capabilities are required for every instance of military operations. Physical shelters can be fixed or transportable in ground mobile, airborne, or shipborne configurations. These shelters may support manned command, control and intelligence (C2I) centers, manned IP or INFO COM centers, or unattended IS resources. Civil IS shelters typically may not involve sleeping quarters or other overnight accommodations but, instead, merely provide facilities housing IS equipment and personnel in common office work environments.

The Cold War era taught that a fixed command center or IS operations building will not survive a determined attack if nuclear weapons are involved. Not even so-called deep underground command centers, regardless of cost, could be certified as survivable. As a result, mobile facilities may be the only viable option in military scenarios where long-term survivability is mandatory. 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 in military, mobile command, surveillance, and IS-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 IOs processing center products to support moving battlefield theater locations. 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.

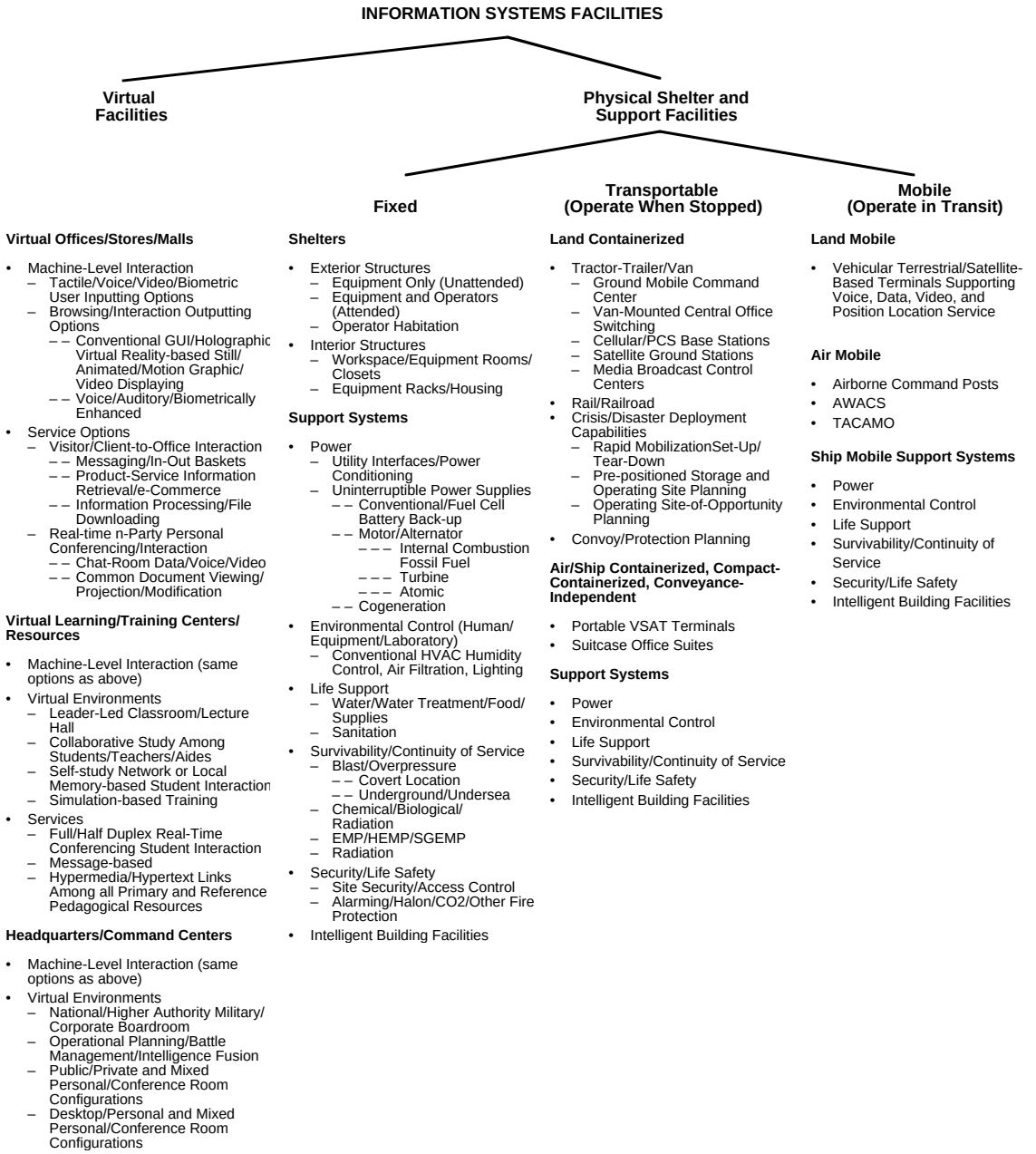


Figure 10.6-1. IS Facilities Capabilities Taxonomy

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, DLC, 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 min 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., 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 PCs 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 highlights examples of currently popular virtual facilities.

RATIONALE

IS facilities intended for human occupation must contain organic security means to identify reliably the people who can enter a facility and to deny access to people who should not enter a facility. In a permissive environment where the people are cooperative, recognition and authorization to enter can be effected by a combination of technologies that depend upon the perceived threat of unauthorized access and its consequences for a system. Security measures are a continuing overhead cost. The degree of security applied must be appropriate to that which is being protected. The technologies used for personnel identification can be flexibly modified, enhanced, or diminished, as threat conditions and missions change. Recognition can be performed by 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 the harmonic content of a human voice; 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 individual physical and physiological properties precludes unauthorized entry because of the difficulties encountered in counterfeiting living biological characteristics. With such security access measures in place, entry will be controlled to attended, remotely attended, or unattended facilities.

Technologies will identify those who should not be admitted to a facility. Identification of attempted unauthorized entry will be specific (e.g., an individual by name, an enemy troop, or even a feral moose or bear). This technology will alert a security team or an assigned tactical reaction force, will provide details of the attempted entry, and will log the event at a different site so that the sequence of events will be preserved if the attempted entry later proves to have been a prelude to destruction or assault. Since actions will be taken confidently based upon this systematic identification process, it must be reliable, with proper safeguards for independent verification.

To protect the facility, the environment inside and outside the facility will be monitored continuously. Sensors for environmental variables will report ambient air and hardware temperatures, humidity, inundation, vibration, fire, barometric overpressure, selected gas partial pressure ratios, chemical agents, movement of people or objects, alternating current (AC) and direct current (DC) bus parameters, coolant failure, and RF activity. This will permit monitoring of facilities too dangerous for human presence or monitoring many areas when insufficient numbers of people

are available to cover all locations. Activities conducted within hostile territory can be monitored remotely through use of such sensor technologies.

Occasions will arise when communications will become necessary between or among people who do not share a common spoken language. The communication process will involve real-time gathering of information concerning each speaker's native language and will be followed by dual-translation activity. Translation modes will be selectable: audio voice, a video narrative display, print, or any combination of these. Language translation capabilities in a variety of languages—to and from English—will be employed. Real-time cross-language conferencing will be conducted in denotative terms without inducing ambiguity. Robotics will be used to perform physical functions, both within the facility and the immediate area. This will provide for protection of a facility located in a hostile environment and not maintained by humans.

The relevance of older military or commercial, high-technology, highly survivable IS facility capabilities in warfare is evident from the preceding discussion. If a potential adversary possesses only fixed IS and support facilities, U.S. and allied precision-guided and other conventional weapons can be effective. In future conflicts, adversaries may have deployed, or will be able to deploy, transportable or mobile IS facilities. 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 needed to target and destroy such a facility. Clearly, the wartime utility of high-technology, high-survivability IS facility capabilities by National Security users must be understood fully by U.S. strategists and planners if effective countermeasures and counterstrike alternatives are to be available.

With the advent of virtual facility technology, the need to concentrate command, surveillance, and intelligence-fusion center facility capabilities in single physical locations is greatly diminished. This means, for example, that target information required by robust, integrated air defense systems does not have to be obtained from radar equipment collocated with, or exclusively dedicated to, the surface-to-air weapons they control. Thus, neutralizing an adversary's air defense surveillance capability may require attacks against non-air defense and potentially non-military active or passive radar facilities and/or IS infrastructures.

Also, since modern teleconferencing nearly eliminates operational penalties associated with distributed or virtual command center designs, transportable or mobile command center elements can be reduced in size, number of people, and complexity. This makes them easier to support and move and, consequently, even more survivable. In the same manner, using distributed-location, virtual fusion centers enhances the integration of tactical-battlefield and strategic-global intelligence and situation assessments, while simultaneously improving overall intelligence-function survivability.

On the economic, commercial, and industrial side, physical and virtual manifestations of IS facilities are increasingly recognized as key competitive factors impacting individual enterprises and the United States' overall position in world markets. As companies streamline operations to stay ahead of rivals, the use of "smart" or "intelligent" building designs to minimize facility and utility costs and the need to provide efficient production, attitude, and morale-enhancing work environments have never been greater.

In the virtual facility arena in particular, the Internet, Intranets (private networks using Internet protocols and software), and supporting technologies and standards are currently able to support myriad forms of e-commerce. In many cases, imaginative entrepreneurs reacting to this "technology push" are creating entirely new and highly successful business ventures and business processes—entities that literally have no precedent. The potential of such groundbreaking endeavors for military use is enormous.

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" interoperation 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:

1. 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.
2. 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.

MCT Part III, Section 3 (Biological Technology), Section 5 (Chemical Technology), and Section 15 (Nuclear Technology) present specific technologies that provide personal and shelter-based protection from biological, chemical, and nuclear weapons effects, respectively.

WORLDWIDE TECHNOLOGY ASSESSMENT (see Figure 10.6-2)

All these IS technology components are or will be available on world markets. Thus, the possibility that potential adversaries will be able to use transportable or mobile IS facilities to mount highly survivable offensives must be fully considered in the planning by U.S. or allied forces.

The United States leads the world in most of these technologies. Robotics technology is being developed and applied in several countries, primarily for repetitive production and manufacturing purposes. Robots capable of performing independent functions are being developed in Canada, Austria, Germany, the United Kingdom, other European countries, and in Japan. There is no clear leader in free-ranging robots outside the U.S. entertainment industry.

In Figure 10.6-2, only 10 of the 38 countries listed have extensive R&D capabilities in all the IS Facilities FA technologies: Canada, Denmark, France, Germany, Japan, Norway, Russia, Sweden, The United Kingdom, and the United States. Several countries have limited capabilities in IS Facilities FA technologies: Iran, Iraq, Libya, North Korea, Poland, and Vietnam.

Country	Virtual Facilities	Fixed Facilities	Transportable Facilities	Mobile Facilities
Australia	●●●	●●●	●●●	●●●
Austria	●●	●●	●●	●●
Belgium	●●●	●●●	●●●	●●●
Canada	●●●●	●●●●	●●●●	●●●●
China	●●	●●●	●●●	●●
Costa Rica	●	●	●	●
Cuba	●	●●	●●	●●
Czech Republic	●	●	●	●
Denmark	●●●●	●●●●	●●●●	●●●●
Egypt	●●●	●●●	●●●	●●
Finland	●●●	●●●	●●●	●●●
France	●●●●	●●●●	●●●●	●●●●
Germany	●●●●	●●●●	●●●●	●●●●
Hungary	●	●	●	●
India	●●	●●	●●	●●
Iran	●●	●●	●●	●●
Iraq	●●	●●	●●	●●
Ireland	●●●	●●●	●●●	●●●
Israel	●●●	●●●	●●●	●●●
Italy	●●●	●●●	●●●	●●●
Japan	●●●●	●●●●	●●●●	●●●●
Libya	●●	●●	●●	●●
Netherlands	●●●	●●●	●●●	●●●
New Zealand	●●●	●●●	●●●	●●●
North Korea	●●	●●	●●	●●
Norway	●●●●	●●●●	●●●●	●●●●
Pakistan	●●	●●	●●	●●
Poland	●●	●	●	●
Russia	●●●●	●●●●	●●●●	●●●●
South Africa	●●	●●	●●	●●
South Korea	●●●	●●●	●●●	●●●
Sweden	●●●●	●●●●	●●●●	●●●●
Switzerland	●●●	●●●	●●●	●●●
Syria	●●	●●	●●	●●
Taiwan - R.O.C.	●●●	●●●	●●●	●●●
UK	●●●●	●●●●	●●●●	●●●●
United States	●●●●	●●●●	●●●●	●●●●
Vietnam	●●	●●	●●	●●

Legend: Extensive R&D ●●●● Significant R&D ●●● Moderate R&D ●● Limited R&D ●

Figure 10.6-2. IS Facilities Technology WTA Summary

LIST OF TECHNOLOGY DATA SHEETS
III-10.6 INFORMATION SYSTEMS FACILITIES

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 III-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.
Technical Issues	Identification accuracy.
Major Commercial Applications	Financial institutions.
Affordability	Other biometric identifiers may become less costly for the reliability offered.

RATIONALE

Finger, thumb, and palm-print identification technologies are closely related to the technologies that appear in the Information Systems Security section (9.4), almost all of which require positive identification of individuals participating in USG and civilian critical IP functions—with a 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 than 1 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, 1 of every 10 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 to 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.

WORLDWIDE TECHNOLOGY ASSESSMENT

Argentina	●●	Australia	●●	Austria	●●●●	Belgium	●●●
Canada	●●●●	China	●	Costa Rica	●●●	Denmark	●●●
Finland	●●●	France	●●●●	Germany	●●●●	Greece	●
Hong Kong	●	India	●●	Iran	●	Ireland	●●●
Israel	●●●●	Italy	●●●	Japan	●●●	Korea	●
Mexico	●	Netherlands	●●●●	New Zealand	●●●	Norway	●●●
Poland	●	Portugal	●	Russia	●●●●	Singapore	●
South Africa Rep.	●●●	South Korea	●●●	Spain	●	Sweden	●●●●
Switzerland	●●●●	Taiwan – R.O.C.	●	UK	●●●●	United States	●●●●
Vietnam	●						

Legend: Extensive R&D ●●●● Significant R&D ●●● Moderate R&D ●● Limited R&D ●

R&D for finger, thumb, and palm-print identification is being done more extensively in countries with a strong military interest or a strong financial interest. Commercially, however, fingerprint identification will be overshadowed by voice identification and other forms of identification more easily handled by telecommunications input.

DATA SHEET III-10.6. WEARABLE COMPUTING SYSTEMS (WCSs)

Developing Critical Technology Parameter	Size; weight; power consumption. Weight is a major factor for Marines since each Marine carries < 100 lbs of equipment.
Critical Materials	Thermal management.
Unique Test, Production, Inspection Equipment	None identified.
Unique Software	Real-time operating systems.
Technical Issues	Response time, signature control, power consumption, heat dissipation, network architecture.
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.

RATIONALE

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 soldier. 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 the soldier's natural remote sensing capabilities with automatic change notification, and instant data access. These characteristics combined allow the soldier to concentrate on mission requirements and not the computer itself.

The WCS will enhance combat effectiveness, act as a force multiplier, and increase soldier survivability. The enabler characteristics of WCS include command, control, communications, and intelligence (C3I); sensor integration providing real-time data for targeting and direction; navigation; threat warning; performance/status monitoring; and supporting missions logistics (eliminate volumes of equipment and documentation) to improve Rapid Deployment Force (RDF) capabilities. Ultimately, WCS will support operational capabilities for NTI/O (e.g., hands-free operation of weapons and equipment); real-time wearable language translation (increasing communication effectiveness during coalition warfare); and GPS/Geographic Information System (GIS) integration (very high resolution).

Integration into soldier systems poses unique technology problems in terms of power consumption (to increase mobility, extend operating life, and decrease logistics load) and thermal management (for soldier survivability, both in terms of the temperature environment and IR signature).

Canada	●●●	Japan	●●●	UK	●●●	United States	●●●●

Legend:	Extensive R&D	●●●●	Significant R&D	●●●	Moderate R&D	●●	Limited R&D	●

Presently, the United States leads in systems integration of WCSs. The state of the art is assembly from COTS components. The technologies for others to build some level of WCSs from components are universally accessible, and a growing body of detailed data on how to assemble a WCS is available on the web. The key discriminators between the state-of-the-art and future developing technologies are size and power dissipation. Advances in these attributes are being made continuously at the component level, with the cost premium required to obtain the state of the art in small size and power consumption being one of the determining factors for component selection.

Developments in component technologies are driven by mass market applications, while interest in true "wearable" computing (as opposed to hand-held computers) is being fostered by groups in academia and vertical markets with specific requirements (e.g., the military).

NRL has just developed and delivered an advanced computer system for the United States Marine Corps (USMC): the enhanced End User Terminal (EUT) for the individual Marine. The EUT is a ruggedized, wearable computer configured on a Modular Lightweight Load-Carrying Equipment (MOLLE) vest. The EUT consists of a full-function Windows NT computer with a Pentium Processor and a touch screen that provides situation awareness to the user and situation reporting to higher level echelons. Complete with a GPS receiver, the user's location is transmitted over an RF link back to headquarters. User locations, locations of other Marines, and threat information are displayed on a 6-in. color liquid crystal display (LCD). The computer system, the GPS, and the RF transmitter are powered form a MIL-SPEC nickel metal hydride (NIMH) battery, which provides approximately 6 hrs. of continuous operation. A recent experiment, Limited Objective Experiment #6) at the Marine Corps Air Ground Combat Center (MCAGCC), Twentynine Palms, California, was the "operational" debut for NRL's EUT. The ability to transmit position reports, situation reports, and other tactical messages, such as "Call for Fire," over a digital link will help reduce the potential for fratricide and increase the warfighters' effectiveness in future combat operations. Planned enhancements will further ruggidize, lighten, and increase the functionality of the EUT. NRL will deliver an additional 10 EUTs for the Marine Corps Warfighting Laboratory experiments scheduled in September 2000 in Gulfport, Mississippi.

MIT is also developing a wearable system [see http://www.media.mit.edu/wearables/ (The MIT Wearable Computing Web Page) or http://vismod/www.media.mit.edu/tech-reports/TR-467/node4.html (Prototype of an Affective Wearable Computer)]. The version of an affective wearable computer that MIT has built uses the PC 104 board standard and private eye display. Attached to this is a medically approved bio-monitoring system made by Thought Technologies. This bio-monitoring system has the ability to monitor simultaneously respiration, galvanic skin response (GSR) (skin conductivity), temperature, blood volume pressure (BVP), heart rate (from BVP), and EMG (electromyogram, for muscular electrical activity). All these can be sensed painlessly from the surface of the skin. Future versions of the system—already under development—include audio and video inputs and displays, wireless links to the Internet, and wireless localized sensors. Current functionality includes the monitoring of four sensors by a Linux-based operating system. The input from the four sensors can be displayed on a text-based screen, such as the Private Eye, with an option for concurrent user annotation. The annotations are automatically time-stamped by the system and stored in a separate log file. In the near future, MIT hopes to add a third log file that will record the user's location at periodic intervals by using GPS for outdoors and a system of fixed IR location broadcasting stations for inside MIT's laboratory.

Core Components

NTI/O is accomplished with either voice or text input. The leading voice recognition engine is based on IBM's Via Voice software. Non-traditional text input is accomplished using a technique called "chording." Chording is the ability to type the complete standard American National Standards Institute (ANSI) text characters by using one hand and not looking at the keyboard. The United States leads in NTI/O technology.

WCS HMD displays are designed to allow the user to interact fully in their normal operating environment. Single-board computers allow for the integration of central processing units (CPUs) and related components onto very small platforms. For comparison, using a single board, a Computer Science professor at Stanford University built a 486-based, 340M hard drive web server that is only 4 in^3 in size (the size of a pack of cigarettes) and runs a full-sized operating system. Japan presently leads the industry in both HMD and single-board computers. Japan leads because of its success in miniature consumer electronics, such as digital cameras and personal music systems. Based on this precursor to success, we can assume that China, South Korea, and Taiwan will soon possess similar capabilities.

Belgium, Canada, the United Kingdom, and other industrialized nations are developing capabilities in both HMD technologies and complete WCS systems integration. The United States leads in integration of COTS components into viable WCS. Several companies sell complete systems. Xybernaut Corporation of Fairfax, Virginia, and VIA Corporation and Interactive Solutions, Inc., of Sarasota, Florida, sell sophisticated WCSs as COTS items for between $3,000 and $5,000.

Presently, cutting edge advances in WCS integration are being driven by the academic community and by demands in vertical markets such as the military. Key academic leaders are Professors Vaughn R. Pratt, Stanford University; Steve Mann, University of Toronto; and Thad Starner, Georgia Institute of Technology. Pratt is the designer of the earlier mentioned web server and developer of tactile "chording" glove. Mann is considered the inventor of WCSs during his 20-year quest to develop something he calls personal imaging, in which an individual wears a camera all the time. Starner, along with Mann, founded the wearable computer project at MIT. The University of Bristol and the University of Essex in the United Kingdom are also key players in WCS systems integration research and offer undergraduate projects in the field. Canada has an active program in wearable computing human systems interface (HIS), which is relevant to this topic. Centers include the University of Toronto and the Memorial University of Newfoundland.

At the critical component level, WCS display technology is a key enabler. Sony, Olympus, and Canon of Japan are leaders in display technology suitable for WCS usage. Liquid Image, in Canada, is developing and marketing state-of-the-art lightweight liquid crystal displays (LCDs) designed for monocular wearable computing applications and for biocular virtual reality (VR). In terms of data presentation, the University of New Brunswick is a recognized world leader in presentation of large data sets of environmental data (e.g., 3-D presentation of bathymetric data).

Epson and Seiko Corporations of Japan are jointly developing the next generation of single-board computers with the capabilities of full-sized systems. The leading fully integrated WCS is the U.S.-based Xybernaut Corporation, Mobile Assistant (MA) II, which features an Advanced Micro Devices, Inc. (AMD) 133MHz, 32 MB Extended Data Out (EDO) Random Access Memory (RAM), 2 GB hard drive and a pair of PCMCIA slots. The MA II is priced at approximately $5,000 and is the result of a joint venture between Xybernaut Corporation and Sony Corporation of Japan.

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 sensing areas of MCTL Parts I and II focus, respectively, on sensing technologies playing vital and critical roles in maintaining U.S. military superiority and those considered sufficient in WMD scenarios. Because the MCT Part III addresses affordability in military as well as economic and INFOWAR operations, 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 section addresses important platform-related sensor requirements, capabilities, and corresponding technology solutions. Using examples, Figure 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, which are important in all military combat scenarios but particularly important for chemical and biological monitoring of environments.

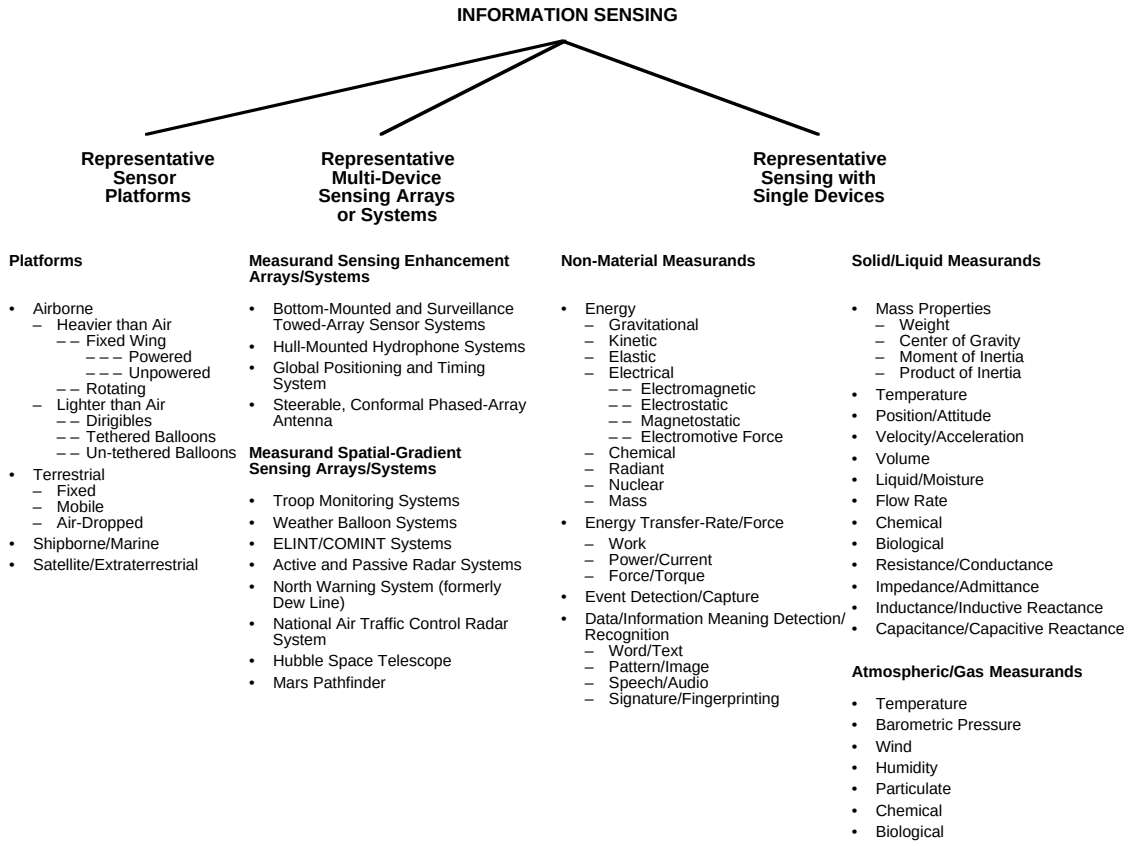


Figure 10.7-1. Information Sensing Taxonomy

The second column from the right depicts measurands associated with non-material entities. This grouping comprises eight kinds of energy,[16] 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, 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

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

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 MCT assessments are, in fact, identified and treated in the tables included in Section 10.3. Likewise, MCT 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 in the MCT 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 Section 10.3.

BACKGROUND

Sensing Technology Description in the MCT

The Information Sensing FA definition at the beginning of this section is formulated to apply universally to all incidences of sensing technology. In developing the definition, it was discovered 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 Figure 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 Figure 10.7-2, a primary iron-constantan[17] 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

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

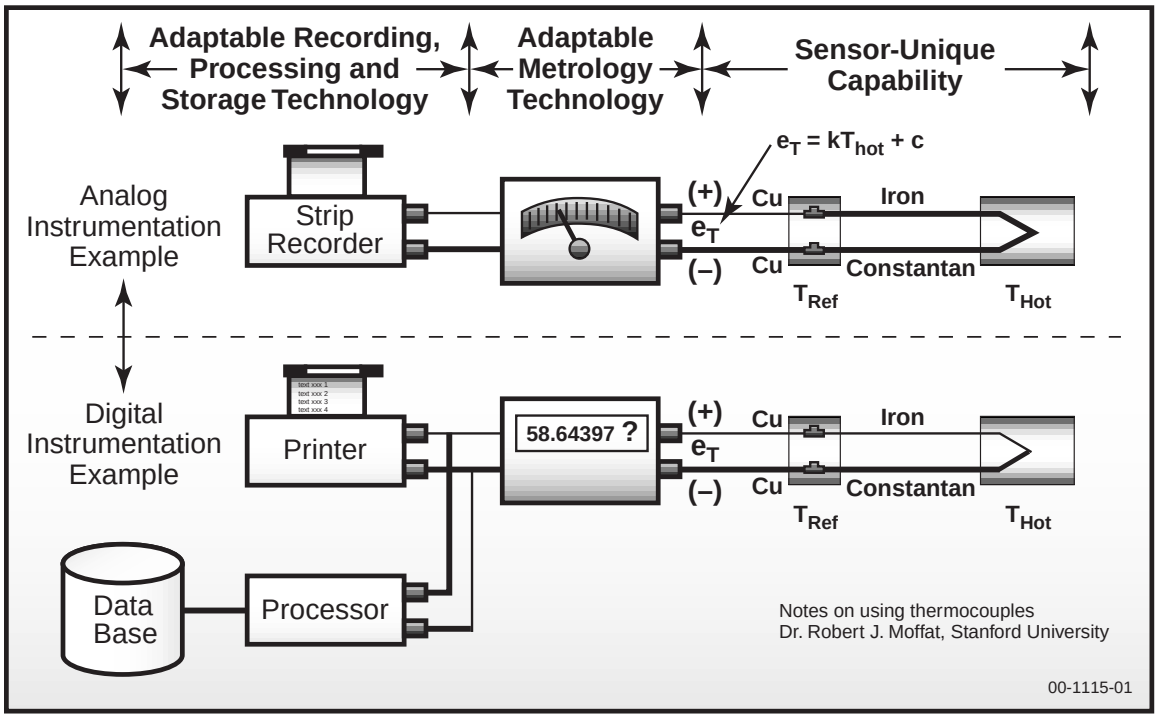


Figure 10.7-2. Thermocouple Example Depicting "Sensor-Unique" Capabilities

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 techniques (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.

While some bimetallic-strip and mercury thermometers directly display temperature readings, the "analog" approach depicted the top half of Figure 10.7-2 uses a "meter" 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:** *Section 12.3, Metrology, assesses measurement technologies for sensor and other applications.*)

The bottom half of Figure 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. To minimize duplication of effort and the possibility of conflicting results from multiple working groups assessing the same technologies, sensor system components have been assigned to the respective list of MCT activities and document sections in which their use and application are dominant. 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 is emerging as another important facet of sensor technology assessment. For instance, fiber-optic-based sensors, while exhibiting significant technical performance advantages over electromechanical and chemical predecessors, continue to be introduced for an ever-expanding number of measurands, with the following products 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.

RATIONALE

Because MCT Part III treats technologies that "produce increasingly superior military performance or maintain superior capability more affordably," both MCTL Part I and Part II sensor technology assessment rationale indirectly

apply to Part III. From the Part I perspective, the truth of this assertion rests in the fact that possessing technologically superior sensors remains a national U.S. military goal. The Part II rationale is applicable for this reason: While sensors are required in most military actions, they are "critical" in chemical and biological warfare.

Part I and II assessment rationale statements are relevant in Part III because any Part III sensing technology that improves superiority or reduces cost could be cause for reassessing that technology in terms of Part I or Part II criteria. Sensing systems that might prove invaluable in warfare but are now prohibitively expensive may be rendered affordable to proliferators by some Part III developing technology. Thus, the Part III "affordability" criteria takes on a much larger significance if it reduces the cost of a particular sensor system *and* enables operations not previously supportable. Parallel arguments also apply to Part I. Should developing technologies reach levels of performance that are used to improve adversary military capabilities, these technologies might challenge or mitigate a U.S. position of superiority. That such capability advances are planned and likely to occur is reflected in the Joint Vision 2010 statement that "new sensors and information dissemination systems will be deployed to detect chemical or biological at great ranges and provide warning to specific units that may be affected."

Beyond Part I- and II-related rationale, a more compelling and far-reaching rationale exists for assessing sensor technology against Part III criteria: In accordance with DODD S-3600.1, assessment must take into account "operations other than war" and the ability to "secure peacetime National Security objectives." The Part III effort must assess sensing technologies by their impact on the conduct of economic warfare and INFOWAR, whether those physical, violence-free campaigns are waged in the midst of or in the absence of military conflict. Sensors must be viewed as key factors in the conduct of economic warfare because they are integral and necessary components of almost every automated industrial process (from basic research; to CAD product development, manufacturing, test, and evaluation; to point of sale retailing; to financial institution, postal and private delivery service document processing; to complex IS continuous or scheduled performance measurement; to numerous others).

While the importance of IP and software is generally taken for granted and the rationale for assessment assumed to be self-evident, it is no exaggeration to state that proper operation and maintenance of these "superpower" technologies is highly dependent upon sensor-based test instrumentation and techniques. Moreover, the information processors and the software directing their operation are powerless to affect the outside world except via appropriate inputting and outputting devices. Figure 10.7-1 (and corresponding figures in other sections containing portions of overall MCTL sensor assessment) identify and describe specific instances of technologies meeting Part III criteria and fulfilling the important National Security functions outlined previously.

WORLDWIDE TECHNOLOGY ASSESSMENT (see Figure 10.7-3)

The United States leads the world in technologies that deal with large amounts of disparate data. Systems that process large amounts of data rapidly and reliably do exist within many national and international financial institutions and telephone systems. These ISs are well organized and used in predictable ways. In the technologies of mathematical modeling and the statistical application of data correlation, Germany, France, the United Kingdom, some other European countries, China, India, and Japan and are also strong.

The basic principles and, increasingly, the components necessary for implementing advanced digital processing techniques are increasingly available. Implementation of militarily critical signal processing functions rests largely on empirically validated target and engineering design databases and empirically optimized algorithms. The United States, by virtue of many years of investment in development, test, and operational use of advanced military sensors, has a significant worldwide lead, and is followed closely by France, Germany, and the United Kingdom. Japan also has all of the underlying technology elements and has developed a variety of military systems (IR sensors, mortar location radars, satellite communications, and so forth) that require state-of-the-art signal processing. Italy, Sweden (airborne radar), and other members of the European Union (EU) have capabilities in specific sensor areas, as do India, Israel, South Africa, and Russia.

Country	Sensor Platforms	Measuring Sensing Enhancement Arrays/Systems	Measuring Statistical Gradient Sensing Arrays/Systems	Non-Material Measurands	Solid/Liquid Measurands
Australia	●●●	●●●	●●●	●●●	●●●
Austria	●●	●●	●●	●●	●●
Belgium	●●	●●	●●	●●	●●
Canada	●●●	●●●	●●●	●●●	●●●
China	●●●	●●●	●●●	●●●	●●●
Costa Rica	●	●	●	●	●
Cuba	●	●	●	●	●
Czech Republic	●	●	●	●	●
Denmark	●	●	●	●	●
Egypt	●	●	●	●	●
Finland	●●	●●	●●	●●	●●
France	●●●	●●●	●●●	●●●	●●●
Germany	●●●	●●●	●●●	●●●	●●●
Hungary	●	●	●	●	●
India	●●●	●●●	●●●	●●●	●●●
Iran	●●	●●	●●	●●	●●
Iraq	●	●	●	●	●
Ireland	●	●	●	●	●
Israel	●●●	●●●	●●●	●●●	●●●
Italy	●●●	●●●	●●●	●●●	●●●
Japan	●●●	●●●	●●●	●●●	●●●
Libya	●	●	●	●	●
Netherlands	●●	●●	●●	●●	●●
New Zealand	●●	●●	●●	●●	●●
North Korea	●	●	●	●	●
Norway	●●	●●	●●	●●	●●
Pakistan	●●	●●	●●	●●	●●
Poland	●	●	●	●	●
Russia	●●●	●●●	●●●	●●●	●●●
South Africa	●●	●●	●●	●●	●●
South Korea	●●	●●	●●	●●	●●
Sweden	●●	●●	●●	●●	●●
Switzerland	●●	●●	●●	●●	●●
Syria	●	●	●	●	●
Taiwan - R.O.C.	●●	●●	●●	●●	●●
UK	●●●	●●●	●●●	●●●	●●●
United States	●●●●	●●●●	●●●●	●●●●	●●●●

Legend: Extensive R&D ●●●● Significant R&D ●●● Moderate R&D ●● Limited R&D ●

Figure 10.7-3. Information Sensors Technology WTA Summary

LIST OF TECHNOLOGY DATA SHEETS
III-10.7. INFORMATION SENSING

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

Bio-Photonic Fluorescent Properties Identification

Chemical Agent Sensors (Variety of Chemicals)

Fast Fourier Transform Analyses Technologies and Implementation

Sensor Management and Integration

Sensor Tasking Algorithms

Sensor Fusion

DATA SHEET III-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.
Technical Issues	Response time, storage design, and network architecture.
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- to 25-year time frame.

RATIONALE

For any system that collects data for military purposes, there is a growing need to protect that data from tampering. The military depends upon the integrity of data used for decision making. This includes data in almost any format: messages, commands, sensor output, photos, audio recordings, videos, web pages, and real-time transmissions.

One of the techniques in information warfare is to distort data upon which decisions are made. In some cases, these attacks will take the form of obvious corruptions (e.g., web pages that have been changed or defaced as a prank or a political statement). Even attacks that appear to be simply malicious can be a means of influence in information warfare (e.g., the bogus news story that affected certain company stock prices). This kind of attack is usually discovered, albeit after some possibly unrecoverable damage has occurred.

In many cases, however, attacks will take the form of subtle changes to critical data—changes unnoticed by humans and contained in vast databases (e.g., changes in map information used for bombing calculations, photos used in news releases in a conflict, wording in diplomatic agreements, and sensor data used to monitor border crossings). The damage from this tampering could range from none to disastrous, depending upon the decisions based upon that data.

Depending on the uses of the data, various levels of tamperproofing protection will be needed, with the greatest protection given to life-critical information (e.g., medical directives for troops in the field or troop locations). Some data will need little protection because of the obviousness of the change. However, almost all data for military use will need some level of protection from tampering. Sensor data will most assuredly need protection from tampering—all the way from collection to transmission to storage to retrieval. Information tamperproofing will be a strong pillar in defensive information warfare.

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. However, the actual development of cohesive methodologies that could be applied to military data is mostly unaddressed.

In the short term, data tamperproofing is more of a problem to the military and certain other critical infrastructure organizations than it is to the commercial market. Even a bank can tolerate some level of tampering since their loss is usually money, the loss of which most large banks have accepted as they would any other fraudulent loss. For the military, however, much more may be at stake.

WORLDWIDE TECHNOLOGY ASSESSMENT

Canada	●●●	Japan	●●●	UK	●●●	United States	●●●●

Legend:	Extensive R&D	●●●●	Significant R&D	●●●	Moderate R&D	●●	Limited R&D	●

Much of the R&D on encryption is applicable for use in information tamperproofing. (See Section 10.4 for more information on this topic.) Some R&D is being done on watermarking (photos in particular) for copyrighting purposes. However, the R&D needs for the military extend far beyond watermarking techniques.

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. This capability will be available for individual or group presentation, without requiring users to have knowledge of the underlying IS structure or internal activities. 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.

RATIONALE

Decision making in a military situation can be based upon manifold, interdependent (although not obviously so) events or situations occurring anywhere in the world. Analyses and correlation of event content may require a search through substantial amounts of data maintained in different formats distributed across memory located in different, geographically distant systems. Decision makers will not be required to be sophisticated technologically or be expected to initiate or define the details of inquiry methodology. Decision support data will be made rapidly available to command authorities. A numeric data credibility level will be declared as a component of the results of each inquiry.

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. Combat is always less than predictable and infested with surprise. 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.

In addition to use in decision making, these presentation capabilities will be used for training and in a variety of other aspects of military preparation.

WORLDWIDE TECHNOLOGY ASSESSMENT (see Figure 10.8-1)

The United States leads the world in most of these technologies. They are primarily resident technologies now being employed throughout the commercial entertainment industry. Exceptions are in the area of VR. Several countries, notably Sweden and the United Kingdom, are also strong in VR technology and implementation.

For integrated distributed visualization and analysis systems [e.g., Multi-dimensional User-oriented Synthetic Environment (μuSE), MUSE Technologies of Albuquerque, New Mexico, is an international leader in the development of perceptual computing software and solutions that help computer users understand complex information by presenting data using sight, sound, and other methods of representation. Users of the μuSE can engage in dynamic collaboration and share insight and information across all types of networks. For additional information on μuSE Software Development Environment 2000, see http://www.musetech.com/index.html).

Country	Sensor Platforms	Measuring Sensing Enhancement Arrays/Systems	Measuring Statistical Gradient Sensing Arrays/Systems
Australia	●●●	●●●	●●●
Austria	●●	●●	●●
Belgium	●●	●●	●●
Canada	●●●	●●●	●●●
China	●●●	●●●	●●●
Costa Rica	●	●	●
Cuba	●	●	●
Czech Republic	●	●	●
Denmark	●	●	●
Egypt	●	●	●
Finland	●●	●●	●●
France	●●●	●●●	●●●
Germany	●●●	●●●	●●●
Hungary	●	●	●
India	●●●	●●●	●●●
Iran	●●	●●	●●
Iraq	●	●	●
Ireland	●	●	●
Israel	●●●	●●●	●●●
Italy	●●●	●●●	●●●
Japan	●●●	●●●	●●●
Libya	●	●	●
Netherlands	●●	●●	●●
New Zealand	●●	●●	●●
North Korea	●	●	●
Norway	●●	●●	●●
Pakistan	●●	●●	●●
Poland	●	●	●
Russia	●●●	●●●	●●●
South Africa	●●	●●	●●
South Korea	●●	●●	●●
Sweden	●●	●●	●●
Switzerland	●●	●●	●●
Syria	●	●	●
Taiwan - R.O.C.	●●	●●	●●
UK	●●●	●●●	●●●
United States	●●●●	●●●●	●●●●

Legend: Extensive R&D ●●●● Significant R&D ●●● Moderate R&D ●● Limited R&D ●

Figure 10.8-1. Information Visualization and Representation Technology WTA Summary

LIST OF TECHNOLOGY DATA SHEETS
III-10.8. INFORMATION VISUALIZATION AND REPRESENTATION

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

Algorithmically Derived Scenarios

Coordinated Distributed Activities (Communications, Database Retrieval, and So Forth)

Cross Section of Images

Distributed Virtual Reality (VR) Scenarios

Group Virtual Reality (VR)

Holography

Presentation Based on Viewer Style

DATA SHEET III-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.
Technical Issues	See Background for amplifying discussion. Ability to fabricate and integrate key elements of circuitry, including internal memory access channels with bandwidths exceeding 10Gbyte/sec and external bandwidths or 3.2 Gbyte/sec or greater. Ability to fabricate high density very large-scale integration/very high-speed integrated circuit (VLSI)/VHSIC chips at .15 micron or lower Effective integration of hardware support for advanced image-generation features, including anti-aliasing, texture and lighting effects, and bump-mapping. Development and implementation of scalable processing techniques and algorithms, especially those based on open standards that might allow the use of low-cost mass market commodity graphics boards in a high performance (> 1.5 Gpixel/sec) system.
Major Commercial Applications	Games, entertainment, including interactive digital video disk (DVD).
Affordability	This technology is likely to be driven by mass market products.

RATIONALE

Augmented-reality displays involving effective integration of live or computer-generated dynamic scenes with knowledge representation from very large data sets will be required to allow the level of battlespace awareness required to achieve information superiority objectives defined in Joint Vision 2010 and Army Vision 2010. To be effective, commanders and other combatant personnel must be able to operate effectively for extended periods of time. One of the key research areas will be the effects (both operational and long-term) of extended use of visually coupled systems.

This critical developing 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.

WORLDWIDE TECHNOLOGY ASSESSMENT

Canada	●●●	Finland	●●	France	●●	Germany	●●
Israel	●	Italy	●	Japan	●●●●	Netherlands	●●
Singapore	●	South Korea	●	Spain	●●	Sweden	●●
UK	●●	United States	●●●●				

Legend: Extensive R&D ●●●● Significant R&D ●●● Moderate R&D ●● Limited R&D ●

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. (See Background for discussion of state-of-the-art and drivers.)

The United States and Japan are world leaders in this technology, which is driven by the commercial sector. Leading firms include nVidia and 3Dfx (in chip technology), Quantum3D (which uses the 3Dfx chips in high-end multichannel systems), and Evans & Sutherland in the area of complete systems. In terms of complexity and performance, the Sony PlayStation2 chipset is the state-of-the-art. The chip set includes a general purpose microprocessor [based on a Multimission Image Processing Subsystem (MIPS) design] capable of delivering 6.2 GFLOPS and a graphics processor chip which U.S. industry representatives have calculated to be capable of 1.2-Gpixels/sec performance. These chips are extremely large (approaching 1 in. on a side) and the advertised price of the complete PlayStation is on the order of $320 U.S. dollars.

Canada (Matrox and ATI) has traditionally been a world leader in this technology. However, based on advertised performance, they appear to be one or two generations behind the world leaders. Similarly, the EU program High Performance Kiosk and Desktop System (HIPER-KIDS) is basically a high-performance rasterizer with limited graphics processing capabilities. This project developed a graphics rasterizer based on Xilinx field programmable gate array chip technology.

A Finnish firm, BitBoys Oy, advertises to have the potential capability to design a state-of-the-art chip that, according to their corporate literature, will be fabricated by Infeon (a spin-off from Seimens). This development is significant because it promises the fastest performance yet indicated (2.4 Gpixels/sec). However, at the current time (January 2000), a lower performance product (advertised as capable of 1.2 Gpixels/sec) is not scheduled for release until spring 2000.)

In France, the INRIA Project SIAMES (Synthèse d'image, animation, modélisation et simulation [trans. Synthesis of image, animation, modeling and simulation) is active in a range of supporting activity algorithm development activities, including state-of-the-art parallel processing techniques.

New developments in DRAM-based technologies provide designers with the opportunity to integrate huge amounts of dynamic random access memory (DRAM), static random access memory (SRAM), and logic on a single chip. The process of embedding logic in DRAMs is being offered by SMST (Germany), a recently established joint venture of Philips (headquartered in the Netherlands) and IBM. In addition, Philips is actively pursuing the development and marketing of graphics processing for DVD applications, such as the TriMedia (TM1300) Programmable Media Processor. This product is aimed at the mass market for multi-media and does not have the performance or functionality of the state-of-the-art graphics processors. However, this product is indicative of a capability.

BACKGROUND

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 (the massive chips used in the Sony Playstation2 being an example.) Recent reports are that the Semiconductor Industries Association (SIA) Road Map accelerates the projected availability of 0.13-micron technology. Two major Taiwanese foundries—Taiwan Semiconductor Manufacturing and UMC Group—are reported to be targeting 2001 for a 130-nm ramp. See Internet web site http://www.techweb.com/wire/story/TWB19991122S0013.

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 that have the experience with and the access to much larger scale VLSI/VHSIC technology.

DATA SHEET III-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.
Technical Issues	Ability to achieve full-immersion for training and/or to enhance operator tactical response—specifically, to match visual acuity with low response time for realistic operator training (see background discussion.). Human factors design and packaging to achieve non-intrusive immersion and response to head and eye movements.
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.

RATIONALE

Significant advances will be required in visually coupled displays to achieve the level of VR required to support future combat mission rehearsal needs. (See Background for discussion of current state of the art and limitations.) The critical developing technologies should provide sufficient fidelity and realism to allow combatants to proceed from training and rehearsal directly to operation without an appreciable recovery time.

In addition, full immersion, when coupled with improved capabilities for and knowledge representation from very large data sets, will allow the level of battlespace awareness required to achieve information superiority objectives defined in Joint Vision and Army Vision 2010. A specific military requirement to which this technology would contribute is in future follow-ons to rapid battlefield terrain visualization Advanced Technology Demonstrations (ATDs) and Advanced Concept Technology Demonstrations (ACTDs).

WORLDWIDE TECHNOLOGY ASSESSMENT

Belgium	●	Canada	●●●●	France	●●	Germany	●●
Japan	●●●	Netherlands	●●	Sweden	●	UK	●●●
United States	●●●●						

Legend: Extensive R&D ●●●● Significant R&D ●●● Moderate R&D ●● Limited R&D ●

Two key global trends are likely to have a dramatic affect on the rate at which technology for immersive displays develops over the next 5 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.

Within the United States, the following organizations are identified as being active in VR display technology:

- University of Washington, Human Interface Technology (HIT) Laboratory
- MIT, Media Laboratory
- University of Illinois/University of Iowa [Cave Automatic Virtual Environment (CAVE)™][18]
- NRL
- Commercial companies (e.g., Barco, Fakespace)
- University of North Carolina [image-based modeling and spatially immersive display (Office of the Future)].

In evaluating worldwide technical capabilities, it must be noted that none of the existing displays, with the possible exception of the CAE Link fiber-optic product, appear to approach the levels defined for the next-generation critical developing technology. The specific products described indicate an investment and position in the market that portend a future potential to advance the state-of-the-art to the critical developing levels identified. Much of the other current research cited tends to be in the areas of supporting image representation and generation and, within the EU, in display materials.

Canada has traditionally been a world leader in this technology. The CAE Link fiber-optic HMD (developed in the early-to-mid 1990s) remains the state of the art. Among the features it provides are full stereo imaging capability and an eye-slaved high-resolution inset in the center of the field of view (2.2 arc-minutes/pixel) and 1.2 million pixels distributed between the inset and the lower resolution (6.0 arc-minute/pixel) in the background. With a 120° H × 55° V field of view, it is also one of the most immersive of the visually coupled subsystems. Canada is also well positioned in the mid-range of products, represented by liquid crystal.

Canada has a strong underlying infrastructure in supporting data visualization and digital scene generation to support applications development. The Human-Computer Interaction Laboratory at the University of New Brunswick is a recognized Center of Excellence for Visualization. Other centers include the Media and Graphics Interdisciplinary Center at the University of British Columbia and the VR group at McGill University.

The United States and Japan have strong efforts in visual display technology. Most of the effort in Japan is aimed at mass market consumer computer and gaming products. The Sony Glasstron is the state-of-the-art for low-cost gaming displays.

Ericcson Saab Avionics of Sweden manufactures an HMD with high resolution (2.5 arc-minutes/pixel) over a 53° H × 41° V field of view. However, the CRT technology used makes for a relatively heavy unit (8 lbs).

Most of the work within the EU ESPRIT and BRITE/EURAM programs is aimed at more conventional displays and on supporting graphics processing and representation techniques required to meet display requirements for a wide range of business, engineering design, and medical applications.

BACKGROUND

The current level of technology for visual VR displays does not adequately support realistic immersion to the point where effective, time-critical combat mission rehearsal can be conducted. Existing combat mission simulation is adequate for general operator training. However, the lack of true stereoscopic immersion and the minute delays in response time caused by processing delay and frame rate create anomalous training effects that may degrade performance if a sufficient recovery time is not allowed between training and live operation.

---

[18] The CAVE is a surround-screen, surround-sound, projection-based VR system. Projecting 3-D computer graphics into a 10’ × 10’ × 9’ cube composed of display screens that completely surround the viewer creates the illusion of immersion. It is coupled with head and hand tracking systems to produce the correct stereo perspective and to isolate the position and orientation of a 3-D input device. A sound system provides audio feedback. The viewer explores the virtual world by moving around inside the cube and grabbing objects with a three-button, wand-like device.

DATA SHEET III-10.8. VIRTUAL REALITY (VR) HUMAN REPRESENTATION

Developing Critical Technology Parameter	Ability to produce realistic avatars of human actors/operators, with sufficient fidelity to allow effective interaction of live human operators and system-generated resources in real-time tactical environments.
Critical Materials	None identified.
Unique Test, Production, Inspection Equipment	None identified.
Unique Software	Specially designed applications software for adapting state-of-the-art image-generation software incorporating "texture and lighting" and bump-mapping capabilities to specific military applications; software models characterizing human physical and behavioral response to military-operations-induced stress.
Technical Issues	Understanding/characterization of human response to military situations and the response of human operators to computer generated avatars; quantification of the potential benefits of using computer-generated avatars in tactical situations; development of specific design criteria and specification for the degree of fidelity in representation required to achieve benefits and meet requirements.
Major Commercial Applications	Commercial applications in gaming and entertainment are driving this technology. The texture and lighting and the bump-mapping features are now standard embedded features of commercial software for mass-market commodity graphics boards for PCs and games.
Affordability	The growing COTS capability will yield affordable hardware. The driving aspect of affordability relates to the potential for increasing crew effectiveness at reduced manning levels.

RATIONALE

R&D activities in tactical decision making and training give strong evidence that human interaction has a significant impact on the effectiveness of INFO EXCH. With increased pressures for lower staffing levels in all aspects of combat, activities are investigating the potential of avatars—computer-generated agents—to help improve the flow of information to increase situational awareness and reduce stress.

Improving the flow of information is a critical aspect of maintaining information superiority and ensuring timely and effective action for precision engagement and full dimension protection as envisioned in Joint Vision 2010. Past events have indicated that, in many cases of combat loss or collateral damage, the systems worked properly (i.e., the targets or threats were correctly sensed and the data presented). The breakdowns that occurred resulted because operators failed to notice or attend properly to the data presented. Introducing the "human" element in the sensor presentation has the potential to increase operator alertness and attention, particularly under information-rich conditions.

Beyond the near-term (5–10 years), improved abilities to model multiple-actor interactions will allow more realistic and effective training—both crew training and command decision making.

WORLDWIDE TECHNOLOGY ASSESSMENT

Czech Republic	●	France	●●●	Germany	●●●	India	●
Israel	●	Japan	●●●	Netherlands	●●	Norway	●
Russia	●	Singapore	●	South Africa	●	South Korea	●
Sweden	●	Switzerland	●●●●	Ukraine	●	UK	●●●●
United States	●●●●						

Legend: Extensive R&D ●●●● Significant R&D ●●● Moderate R&D ●● Limited R&D ●

Activity in this technology is driven increasingly by a combination of a demand for improved realism and fidelity in computer-generated characters for gaming and entertainment and a growing availability of technology and university programs in human performance modeling. The activities and organizations cited are examples and do not constitute a comprehensive or exhaustive listing.

Military research in the United States includes

- Activities at NRL
- The Computerized Anthropometric Research and Design Laboratory and the Crew System Ergonomics Information Analysis Center (CSERIAC) at the Wright Patterson Air Force Base, Ohio
- The U.S. Army Research Laboratory (ARL) Survivability/Lethality Directorate work in modeling of casualties
- Space and Naval Warfare Systems Command (SPAWAR) Systems Division San Diego, work in Tactical Decision-Making Under Stress (TADMUS), while not directly related, has relevant research relating to human operator response to voice input.

Other efforts identified in the United States include:

- **George Washington University.** National Crash Analysis Center (NCAC). The NCAC is a Federal Highway Administration (FHA)-funded research center concentrating in Human Modeling/Occupant Safety vehicle crashworthiness research http://www.ncac.gwu.edu/
- **Georgia Tech.** work in simulating Human Motion http://www.cc.gatech.edu/gvu/animation/Areas/humanMotion/humanMotion.html
- **New York University.** Media Research Laboratory and the Improv Project, a system for real-time animation of behavior-based Interactive Synthetic Actors (http://www.mrl.nyu.edu/improv/index.html)
- **University of Pennsylvania, Department of Computer and Information Science, Center for Human Modeling and Simulation**. This department conducts research in modeling and animation of human movement and related research ranging from image synthesis to natural language interfaces. Applications include MediSim, and JACK, a 3D interactive environment for controlling articulated figures featuring a detailed human model that includes realistic behavioral controls, anthropometric scaling, task animation and evaluation systems, view analysis, automatic reach and grasp, collision detection and avoidance, and many other useful tools for a wide range of applications.

Among foreign activities, the following are highlighted:

- **University of Geneva, MIRALab (**http://miralabwww.unige.ch/). The MIRALab research group at the University of Geneva was founded in 1989 by Nadia Magnenat-Thalmann (one of the world leading experts in the field of virtual humans and virtual worlds). It includes VR, computer animation, and telerobotics work

  A key objective of the lab is to assemble researchers from several disciplines (computer science and electrical engineering, physics and mathematics, networking and multimedia, architecture and design, psychology, videoart, and so forth) and to forge links between them in a broad effort to understand human functionality and to simulate it in a realistic way. An important policy is to work toward their research goals in the context of productions accessible to the general public—not just demos but interactive shows where the audience is entertained while being brought up to date on technical innovations, and can judge and react.

  The general research areas at MIRALab include the design of networked virtual worlds, real-time recognition of emotions and interactive reactions of virtual humans through emotional models, rapid photograph-based cloning techniques that allow simulation of facial expressions, and direct communication between real and virtual humans using speech, emotions, and facial expressions.

  The group also specializes in the simulation of physics-based deformable models, such as clothing and hair. Other work focuses biomechanical models in the simulation of wrinkles and the aging process.

Approximately one third of the research is dedicated to medical informatics, including topological models for the reconstruction of muscles, bones and skin, as well as simulation processes.

MIRALab is funded largely through its intensive participation in several European projects and its collaborations with the private sector. Much of the fundamental research is supported as part of the Swiss National Research Projects.

- Loughborough University (Leicestershire, United Kingdom) has a program, Human Measurements, Anthropmetry and Grow Research Group (HUMAG) at the Department of Human Sciences. The major objective of HUMAG is to promote and pursue applied research in human structure, growth, and function and to develop techniques relevant to this purpose (e.g., the novel 3-D whole body scanner). The organization and undertaking of anthropometric survey work has been a prominent feature of this group's activities.
- **University of British Columbia (Canada)**. The university's FaceMaker is based on a hierarchical spline modeler, called the "dragon editor." It is a WWW front end to the animation subsystem, and does not incorporate interactive modeling tools (see http://zeppo.cs.ubc.ca:5656/)
- **Laboratoire d'infographie (LIG)/Ecole Polytechnique Féderalé de Lausanne (EPFL).** The Computer Graphics Lab (LIG) at the Swiss Federal Institute of Technology (EPFL) in Lausanne was founded in July 1988. The laboratory is mainly involved in computer animation and VR. LIG is especially well-known for the creation and animation of virtual actors. Research is oriented towards virtual humans in virtual worlds. Researchers model body and face surfaces, and then motion is generated based on physical laws, AI, and behavioral laws. Efforts include models for walking, grasping, motion synchronization, collision detection and perception. Also included is work on more complex models based on muscular mechanics for medical applications. Researchers are investigating techniques of VR and real-time interaction to allow the immersion of the user in these virtual worlds and the use of gesture-based commands, interactive physical deformations, and shared virtual environments.

SECTION 10.9—MODELING AND SIMULATION

Highlights

- To assist human decision makers, models based upon behavioral characteristics of psychological and social disciplines will be developed.
- 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.
- Every military system will be aided by simulation, either to expand the capability of the human user or to replace entirely certain functions that were 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, which generically includes concepts such as a business model, a toy, advocated behavior, or someone displaying clothing fashions. 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. Uncritical or complacent acceptance of system-generated wisdom is not recommended. Blind faith in a system can result in military tragedy.

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 testing, validating, or assessing security of other systems. Essentially, every military system will be aided by simulation, either to expand the capability of the human user or to replace entirely certain functions that were previously performed by a human user.

Simulation will aid in policing ISs for 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.

RATIONALE

There will be an enduring need for real-time gathering of information that requires ongoing, specialized analyses. Analytic performance will be structured upon formally requested information and upon algorithmically derived scenario generation. An IS will be able to present a rational projection of consequences and requirements of courses of action currently being considered, integrating both tactical and logistic factors. For example, the viewer of a status condition or inquiry can be presented with information germane to the current course of action or with particulars essential to a current decision process, based upon algorithmically derived options and limitations.

Modeling support to these simulations will require the use of several disciplines not conventionally associated with IS operations activities. To represent the human decision maker and social and group behavior, models based upon psychological and social disciplines will be developed.

Simulations will contain sufficient logic to collect, analyze, and present information automatically and in such a manner that the user has confidence in the analyses and representations being presented or displayed. The underlying ISs will have a built-in capability for automated self-protection, automated maintenance and repair, and automated disaster detection and recovery. All this will be done in a reliable, self-correlating, and automatic deconflicting manner. Processing and presentation will be sufficiently rapid and responsive to permit multiple users to work interactively, or in isolation, simultaneously on the same problem in a coordinated fashion (e.g., in a war gaming situation).

WORLDWIDE TECHNOLOGY ASSESSMENT (see Figure 10.9-1)

The United States leads the world in most of these technologies. Strength in M&S also exists in Germany, France, Japan, Russia, and the United Kingdom. Japan is particularly strong in use of simulating processes.

Country	Modeling and Simulation
Australia	●●●
Austria	●
Belgium	●
Canada	●●●
China	●
Costa Rica	●
Cuba	●
Czech Republic	●
Denmark	●
Egypt	●
Finland	●
France	●●●●
Germany	●●●●
Hungary	●
India	●
Iran	●
Iraq	●
Ireland	●
Israel	●●
Italy	●
Japan	●●●●
Libya	●
Netherlands	●
New Zealand	●
North Korea	●
Norway	●
Pakistan	●
Poland	●
Russia	●●●●
South Africa	●
South Korea	●
Sweden	●
Switzerland	●
Syria	●
Taiwan - R.O.C.	●
UK	●●●●
United States	●●●●

Legend: Extensive R&D ●●●● Significant R&D ●●● Moderate R&D ●● Limited R&D ●

Figure 10.9-1. Modeling and Simulation Technology WTA Summary

LIST OF TECHNOLOGY DATA SHEETS
III-10.9. MODELING AND SIMULATION

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

Biological and Psychological Models

Cross Section of Images

Mathematical Modeling of Behavior

Multi-resolution Modeling

Natural Environment Modeling

Virtual Prototyping Modeling

DATA SHEET III-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.
Technical Issues	Wide variability and lack of subject uniformity and subject response to different conditions.
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.

RATIONALE

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. As a result, the actions are either sub-optimal (i.e., the random or scripted selection may not reflect the optimal decisions that a human operator would make) or predictable (i.e., more easily circumvented by human operators).

Current simulated forces behave unrealistically and lack higher cognitive capabilities. The opportunity exists to:

- Exploit novel architectures and knowledge representation schemes to improve model robustness and capability
  - Inject optimization techniques, such as genetic algorithms and neural networks
  - Explore applications of fuzzy logic fuzzy neural systems already proven effective in high-level robotic control
  - Inject realistic behavior modulator (e.g., fatigue) effect
- Adopt integrated architectural approaches to improve model cognitive skill, scalability, flexibility, and usability at the individual, team, and organizational levels.

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 range of 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 for mission planning and rehearsal and operational C4I2 support.

France	●●●	Germany	●●	Italy	●	Netherlands	●●
Russia	●●	Switzerland	●●●	UK	●●●●	United States	●●●●

Legend: Extensive R&D ●●●● Significant R&D ●●● Moderate R&D ●● Limited R&D ●

The United States has the largest body of research directed toward CGAs for military M&S; however, modeling of human behavior is an area of widespread academic research. Much of this work is focused on meeting the objectives of the Synthetic Theater of War (STOW). In the United States, key players in the area of CGAs include the NASA Virtual Environment Technology Laboratory, University of Houston, U.S. Army Simulation, Training, and Instrumentation Command (STRICOM), and related work at the University of Central Florida in Orlando, which is a recognized Center of Excellence for M&S.

The Advanced Distributed Simulation Research Consortium (ADSRC), consisting of Grambling State University, Florida A&M University, the University of Houston, and the University of Central Florida, conducts research in the application of parallel and distributed evaluation, visualization, and AI reasoning to advanced distributed interactive simulation (DIS).

Other activities identified include those at the Navy Center for Applied Research in Artificial Intelligence (NCARAI) at NRL, the Air Force Institute of Technology (AFIT), and University of Michigan (Soar)[19]. The Soar Intelligent Forces (IFOR) effort is a collaborative effort between researchers at the Carnegie Mellon University (CMU) School of Computer Science, the University of Michigan's Artificial Intelligence Laboratory, NCARAI at NRL, and the University of Southern California's Information Sciences Institute.

The European Institute of Cognitive Sciences and Engineering (EURISCO) in Toulouse (France), the University of Amsterdam in the Netherlands, and the School of Computer Science University of Birmingham Cognitive Science Research Centre in the United Kingdom have programs in modeling of human behavior.

The objective of the United Kingdom's University of Cambridge cognition and emotion program is to develop a theoretical understanding of the nature of emotion and of the cognitive (e.g., attention, interpretation, memory) and brain processes that support normal emotional behavior and response, as well as emotional disorders. The Geneva Emotion Research Group is part of the Faculty of Psychology and Education Sciences at the University of Geneva and conducts emotions research, including experimental studies on emotion-antecedent appraisal, emotion induction, and physiological reactions to emotional behavior in autonomous agents. While this work is primarily directed toward modeling and understanding of individual and group interactions in civilian settings, the underlying data and techniques should be transferable to military scenarios.

19 Soar is a mature, state-of-the-art AI architecture conceived in the early 1980s.

DATA SHEET III-10.9. DETERMINISTIC MODELING

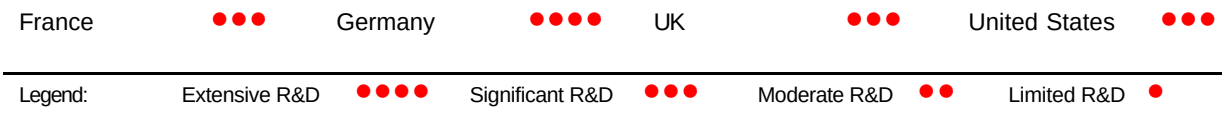
Developing Critical Technology Parameter	Use of deterministic models to characterize and/or predict performance of complex non-linear systems of multi-element forces in tactical environments.
Critical Materials	None identified.
Unique Test, Production, Inspection Equipment	None identified.
Unique Software	Specially-designed software and algorithms for effective modeling of chaotic behaviors of complex, non-linear systems.
Technical Issues	Because of the inherent nature of chaos and non-linear systems in linkages between computer simulation, deterministic model equations and natural phenomena can break down at virtually any arbitrary scale.
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.

RATIONALE

Deterministic models can be used to represent heterogeneous force structures and terrain, such as obstacles, gradients, and so forth. One example, Oak Ridge National Laboratory's DCOR,[20] has been stated to accurately compute a variety of maneuvers including splitting, turning, and regrouping, among others. This program has also been benchmarked against results of staggered defense scenarios to verify its accuracy. Visualization and animation techniques have been developed to reduce the complexity and sheer size of the generated data to graphical depictions easily comprehendible by the user.

Benefits of deterministic modeling include efficient use of human resources by simplifying input preparation and output interpretation; efficient use of computational resources; rapid execution of sensitivity analyses for optimal strategy ("what if" scenarios); and versatility resulting in quick adaptation of the code to more general and even non-military competitive situations (e.g., economic competition, coalitions, low intensity conflict, and so forth).

WORLDWIDE TECHNOLOGY ASSESSMENT



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. The Society for Computer Simulation International (SCSI) boasts worldwide participation. Among the activities of interest (as a measure of globalization), SCSI has established a "virtual" institute, the McLeod Institute of Simulation Sciences, whose purpose is to promote the advance and dissemination of M&S technology. International institute members include:

- Belgium: University of Ghent

---

20 DCOR is a deterministic combat model code (see http://nas.cped.ornl.gov/nas-codes/docr.html).

- Canada: the University of Calgary, Laurentian University, and the University of Ottawa
- Germany: Technical University of Clausthal
- Hungary: Hungarian Academy of Sciences
- Italy: National Research Center (CNR)
- Latvia: Riga Technical University
- Mexico: Universidad Panamericana; China-Beijing University of Aeronautics and Astronautics
- Poland: Polish Academy of Sciences
- Scotland: University of Edinburgh
- United Kingdom: De Montfort University.

DATA SHEET III-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.
Technical Issues	Monitoring and control of sequencing and dependencies among multiple discrete events and characterization and assurance of processes between discrete events, particularly for complex systems in environments whose characteristics are not well-ordered or predictable.
Major Commercial Applications	Process control and transportation modeling.
Affordability	None identified.

RATIONALE

The purpose of a DE simulation is to study a complex system by computing the times that would be associated with real 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 alternative battle management options to optimize force and weapon assignments.

Turnaround time increases with the level of fidelity in each entity or increased number of entities and/or longer simulation time in the scenario. The critical technology for solving this shortfall is to apply parallel processing techniques, such as optimistic parallel processing.

WORLDWIDE TECHNOLOGY ASSESSMENT

Australia	●●	China	●	France	●●●	Germany	●●●●
Russia	●●	UK	●●●	United States	●●●●		

Legend: Extensive R&D ●●●● Significant R&D ●●● Moderate R&D ●● Limited R&D ●

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. As with other aspects of M&S, international interest in DE modeling is extensive.

Centers of Excellence identified in the United States include Virginia Tech University, the University of Central Florida, Syracuse University, the University of Arizona, the University of Florida, and the University of California Berkeley. Also for DE simulations, much research is being conducted and much expertise resides in U.S. DoD

Laboratories [e.g., NRL, the Naval Surface Warfare Center (NSWC), the Naval Air Warfare Center (NAWC), the Naval Undersea Warfare Center (NUWC), ARL, the Air Force Research Laboratory (AFRL), the Army Concepts Analysis Agency (CAA) and so forth] and in Federally Funded Research and Development Centers (FFRDCs) [e.g., RAND Corporation, the Institute for Defense Analyses (IDA), the Center for Naval Analyses (CAN), and so forth).

European sites identified as doing work in DE modeling include the Université de Bretagne Occidentale in France and the University of Magdeburg in Germany. Several universities and private concerns in the United Kingdom are also active in this area, primarily as a tool for structured systems analysis and design.

DATA SHEET III-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.
Technical Issues	Real-time management of distributed networks and routing and local storage of critical information resources, particularly in video resource-intensive environments.
Major Commercial Applications	M&S of distributed industrial and business enterprises.
Affordability	Ability to model and verify operational characteristics of geographically dispersed units provides major cost savings over traditional field exercises.

RATIONALE

In considering this subarea, it is useful to distinguish between the formal standard called DIS (Distributed interactive simulation), which is a mature and relatively limited technology, and critical developing technologies for distributed simulation. Ultimately, the use of DIS is envisioned as improving force readiness and effectiveness by allowing forces stationed in geographically dispersed locations to train together in a realistic, many-on-many environment. As implied in the entry under technical issues, distribution of knowledge about the entities is critical. Older DIS standards assume distribution of the complete database to all entities before the simulation starts. Ultimately, something more robust will be required (e.g., allowing dynamic accessing of knowledge from other entities in the simulation as well as global information about the battlespace environment and the state of other players).

WORLDWIDE TECHNOLOGY ASSESSMENT

Australia	●●●	France	●●●	Germany	●●	Italy	●●
Netherlands	●●	Switzerland	●●●	UK	●●●●	United States	●●●●

Legend: Extensive R&D ●●●● Significant R&D ●●● Moderate R&D ●● Limited R&D ●

The United States is a world leader in this area, and the HLA and RTI have emerged and are becoming widely accepted as de facto standards for distributed simulation by the international community. Even though the United States has made strides in distributed simulation technology and HLA had provided a great leap in capability, many shortfalls still exist in distributed simulation, such as lack of:

- Robust time management
- Multi-level security
- Data servers
- Federation verification, validation, and authentication (VV&A)

- Real-time support
- Consistent natural environment representation, interpretation, and calculation and translation of the environmental effects in different simulations in a federation.

Examples of global research in the development and application of HLA include work at the Interactive Information Institute, Royal Melbourne Institute of Technology, a cross-faculty institute that is becoming a major base for simulation technology research in Australia. The Distributed Knowledge Processing Group at the United Kingdom's University of Surrey is also actively pursuing techniques for distributed simulation. In Germany, the University of Magdeburg, the University of Hamburg, and the German National Research Center for Information Technology are also active in this area.