SECTION II

INFORMATION SYSTEMS TECHNOLOGY

SECTION 2—INFORMATION SYSTEMS TECHNOLOGY

Scope

BACKGROUND

There are many different definitions for Information Systems (IS). The following definition is used for Part II:

> *People, technologies, and machines used to capture or generate, collect, record, store, retrieve, process, display and transfer or communicate information to multiple users at appropriate levels of an organization to accomplish a specified set of functions.*

This definition suggests the wide range of technologies incorporated in different Information Systems.

Since Information Systems are likely to be used in most WMD weapons systems, this separate IS section promotes a more consistent, thorough, and effective assessment. These assessments emphasize countries, other than the United States, which might be adversaries. Consideration is also given to coalition arrangements for both adversaries and allies. Enabling IS capabilities relevant to subnational activities are treated insofar as those activities might target nations or nation-states.

Subsets of Information Systems are commonly referred to as Functional Areas. A large information system may have as many as seven functional areas. IS requirements are normally allocated to functional areas (or system segments). For instance, functional area specifications allow system architects to select the best hardware or software implementation solutions available at the time of fabrication and production. Specifications written in terms of bandwidth, signal quality, reliability, availability, and other generic performance parameters leave designers free to make optimum selections. In the media area, for example, metallic or fiber-optic cable or satellite or terrestrial radio can be selected depending on the speeds and accuracies specified as requirements.

Highlights

- Information Systems capabilities, built on the grid of existing military and commercial technologies, enable most WMD operations
- Large damage envelopes of WMD minimize precision weapon guidance, delivery, and information systems dependencies.
- Information Systems (in some form) can be anticipated to be used by most proliferators.

Assessing technologies in terms of IS functional area capabilities, as opposed to specific hardware/software composition, minimizes the requirement for revised MCTL assessments as new products or devices are introduced or older ones withdrawn. For example, a new WMD weapon delivery or damage assessment requirement might be discovered for real-time video observation of battlefield or target areas at a remote command center. If no prior real-time video requirement existed in a proliferant's information systems, then in all likelihood channel bandwidth or bit-rate revisions to the Information Communications functional area capability parameters would be necessary. A real-time observation capability would mean that there is possession of or access to guided or unguided (terrestrial or satellite, radio or optical transmission through the atmosphere or outer space) media technology, with the ability to support video traffic.

Figure 2.0-1 illustrates the extensive scope of what qualifies as an information system and shows the seven traditional functional areas: (1) Information Processing, (2) Information Security, (3) Information Exchange, (4) Information Communications, (5) Information Management and Control, (6) Information Systems Facilities, and (7) Information Systems Sensors. The information system examples in Figure 2.0-1 include large, complex entities such as enterprise management information systems (MIS), telecommunications systems, and even the worldwide Internet. The list could be extended to include numerous smaller systems such as those based on personal computers.

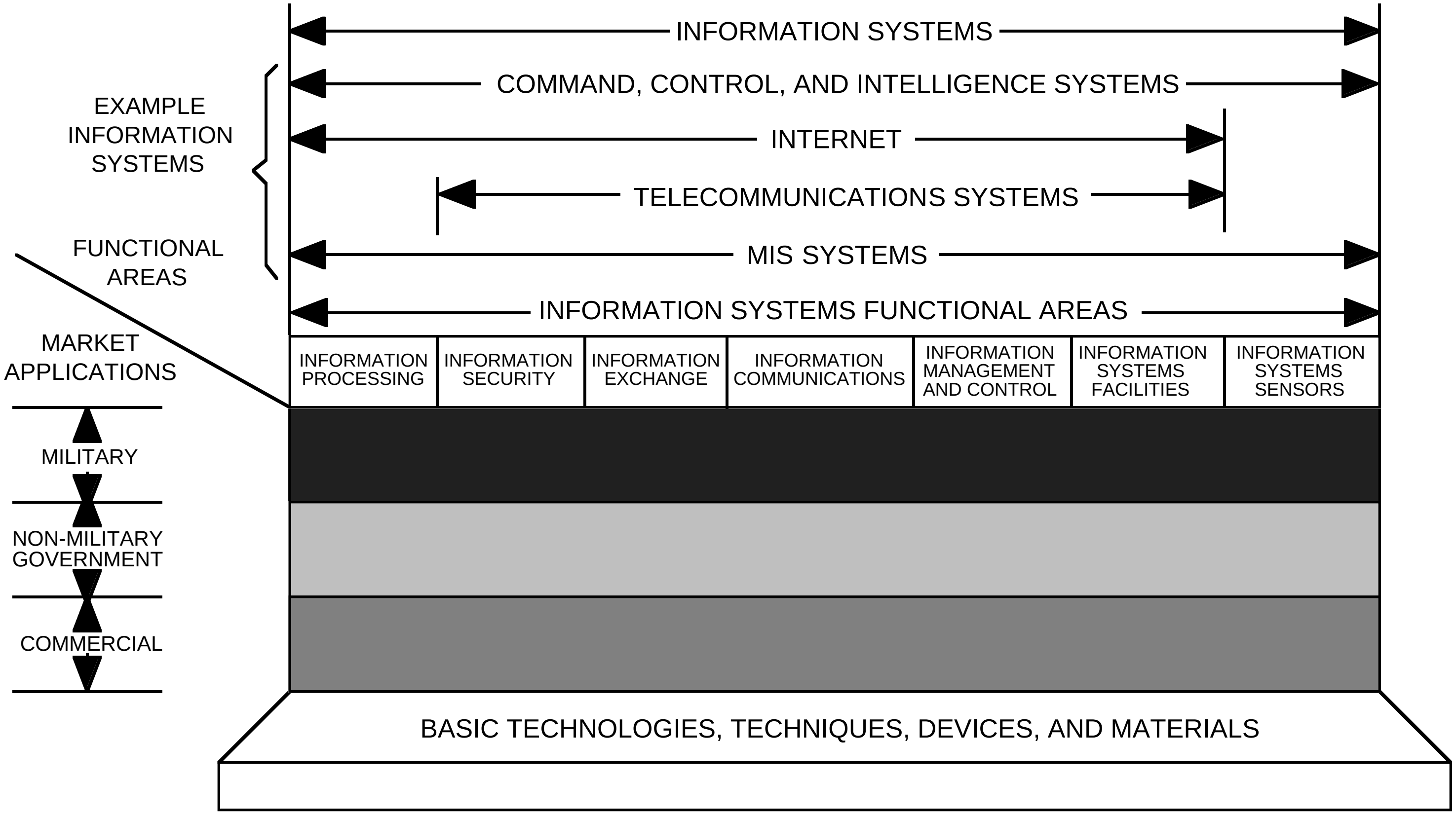
INFORMATION SYSTEMS
EXAMPLE INFORMATION SYSTEMS
COMMAND, CONTROL, AND INTELLIGENCE SYSTEMS
INTERNET
TELECOMMUNICATIONS SYSTEMS
FUNCTIONAL AREAS
MIS SYSTEMS
INFORMATION SYSTEMS FUNCTIONAL AREAS
MARKET APPLICATIONS
INFORMATION PROCESSING
INFORMATION SECURITY
INFORMATION EXCHANGE
INFORMATION COMMUNICATIONS
INFORMATION MANAGEMENT AND CONTROL
INFORMATION SYSTEMS FACILITIES
INFORMATION SYSTEMS SENSORS
MILITARY
NON-MILITARY GOVERNMENT
COMMERCIAL
BASIC TECHNOLOGIES, TECHNIQUES, DEVICES, AND MATERIALS

Figure 2.0-1. Information Systems

OVERVIEW

This section identifies IS technologies that have potential utility in implementing and enabling critical WMD operations. Of special interest in this section are Information Systems built on the grid of existing technologies, including those of World War II vintage, as opposed to those depending on development that requires an extensive industrial base. In particular, this section focuses on the minimum set of technologies required for the development, integration, or employment of WMD and their means of delivery. This is in contrast with Part I of the MCTL, in which performance levels ensuring superiority of U.S. military systems were provided.

In Part II, the innovative use of commercial-off-the-shelf (COTS) technology, perhaps in combination with advanced and older military IS technologies, dominates the assessments. In this COTS category are systems that are procured for civilian purposes, which are rapidly re-programmable for military operations. Modern, fiber-optic-based, software-defined telecommunications networks are a prime example. Properly designed, they provide multimedia voice and data service to the general population and can also constitute a highly survivable backbone for equipment that is optimized for military operations.

IS functional areas for WMD capabilities often overlap those cited in MCTL Part I, Section 8. They differ principally in that performance levels ensuring superiority of U.S. systems are not imposed. However, MCTL Part I provides complementary technical assessment information.

RATIONALE

Recent experience demonstrates the value of both military and commercial IS techniques. Unlike the past when DoD, NASA, and other USG agencies dominated and sponsored frontier developments, the vast majority of technologies supporting today's information systems are driven by civil requirements. Increasingly, the government is specifying "off-the-shelf" mainstream commercial "open-systems, standards-based technologies" as the method of choice for avoiding obsolescence in a fast-changing technology environment.

Overall, strategic and tactical military use of information systems encompasses a range of applications from wide-area switched networks serving an entire theater of operations (often countrywide with global interties), to local processing and communications systems including transportable and personal hand-held devices, to IS systems embedded in smart weapons and sensors. Proliferator possession of critical technologies supporting such a diversity of applications can have decisive significance. In areas of direct combat support, information systems sustain the performance advantages of management, command and control, surveillance, and guidance and control systems for weapons of mass destruction.

It should be noted that most of the technology capabilities cited are those that could be of interest to proliferant countries with large numbers of weapons and relatively capable delivery systems. Countries with fewer resources may employ their weapons with minimal IS support. In fact, one reason why WMD are appealing to even subnational groups is that their large damage envelopes and lethal radii reduce the need for precision weapon delivery and other IS dependencies.

In many cases, U.S. military countermeasure capabilities and techniques may be ineffective when used against commercial IS systems. For example, it may be extremely difficult or impractical to successfully electronically jam large metropolitan area cellular communications systems or all commercial satellite systems that an adversary may have at its disposal.

The tables in this section that identify technologies should be interpreted in the following manner. Proliferants with only a small number of WMD and no intention or capability of sustaining a long-term WMD attack may not be strongly dependent upon the availability of any supporting IS technology. When IS technology is required or helps facilitate WMD, under the column titled "Sufficient Technology Level," the statement depicts technology items that meet most requirements identified during analysis of the wide range of WMD scenarios considered in this document. For COTS technology items, the statements generally indicate that commercial-application performance requirements for capacity, service, quality, availability, etc., generally exceed those encountered in WMD application scenarios.

FOREIGN TECHNOLOGY ASSESSMENT (See Figure 2.0-2)

The United States currently leads in system engineering and integration of complex information systems, closely followed by the UK, France, Germany, Canada, and Japan. Underlying technologies for Information Systems and wide-area integration of such systems are driven largely by commercial requirements. A significant number of countries have developed capabilities equivalent to those of the United States in network switching and transmission. 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 MCTL Part I).

While the United States continues to be the only country with critical capabilities in all IS technology Functional Areas (FAs), equivalent capabilities are found in one or more other countries in every FA. The growing multi-nationalization of information systems developments has increased the worldwide availability of advanced IS technologies. U.S. technology leadership in communications and computer systems has declined in recent years relative to Europe and Japan.

Country	Sec 2.1 Information Communications	Sec 2.2 Information Exchange	Sec 2.3 Information Processing	Sec 2.4 Information Security	Sec 2.5 Information Systems Management and Control	Sec 2.6 Information Systems Facilities
Australia	♦♦♦♦	♦♦♦♦	♦♦♦	♦♦♦♦	♦♦♦	♦♦♦
Canada	♦♦♦♦	♦♦♦♦	♦♦♦♦	♦♦♦♦	♦♦♦♦	♦♦♦♦
China	♦♦	♦♦	♦♦♦	♦♦	♦♦	♦♦
Cuba	♦♦	♦♦	♦♦	♦♦	♦♦	♦♦
Czech Republic	♦♦	♦♦	♦♦	♦♦	♦♦	♦♦
Denmark	♦♦♦♦	♦♦♦♦	♦♦♦♦	♦♦♦♦	♦♦♦♦	♦♦♦♦
Egypt	♦♦	♦♦	♦♦	♦♦	♦♦	♦♦♦
Finland	♦♦♦♦	♦♦♦♦	♦♦♦	♦♦♦♦	♦♦♦	♦♦♦
France	♦♦♦♦	♦♦♦♦	♦♦♦♦	♦♦♦♦	♦♦♦♦	♦♦♦♦
Germany	♦♦♦	♦♦♦♦	♦♦♦♦	♦♦♦♦	♦♦♦♦	♦♦♦♦
Hungary	♦♦	♦♦	♦♦	♦♦	♦	♦♦
India	♦♦	♦♦	♦♦♦	♦♦♦	♦	♦♦
Iran	♦	♦	♦♦	♦♦♦	♦	♦
Iraq	♦	♦♦	♦♦	♦♦	♦	♦
Israel	♦♦♦♦	♦♦♦	♦♦♦	♦♦♦♦	♦♦♦♦	♦♦♦
Italy	♦♦♦	♦♦♦	♦♦♦	♦♦♦	♦♦♦	♦♦♦
Japan	♦♦♦	♦♦♦♦	♦♦♦♦	♦♦♦♦	♦♦♦♦	♦♦♦♦
Libya	♦	♦	♦	♦	♦	♦
North Korea	♦	♦♦	♦♦	♦♦♦	♦	♦
Norway	♦♦♦♦	♦♦♦♦	♦♦♦♦	♦♦♦♦	♦♦♦♦	♦♦♦♦
Pakistan	♦	♦	♦♦	♦♦	♦♦	♦♦
Poland	♦♦♦	♦♦	♦♦	♦♦	♦♦♦	♦
Russia	♦♦	♦♦♦	♦♦♦	♦♦♦	♦♦	♦♦♦
South Africa	♦♦♦	♦♦♦♦	♦	♦	♦	♦
South Korea	♦♦♦	♦♦♦	♦♦♦	♦♦♦♦	♦♦	♦♦♦
Sweden	♦♦♦♦	♦♦♦♦	♦♦♦♦	♦♦♦♦	♦♦♦♦	♦♦♦♦
Switzerland	♦♦♦♦	♦♦♦♦	♦♦♦	♦♦♦♦	♦♦♦	♦♦♦
Syria	♦♦	♦♦	♦♦	♦♦	♦♦	♦♦
Taiwan	♦♦♦♦	♦♦♦	♦♦♦	♦♦♦	♦♦♦	♦♦♦
United Kingdom	♦♦♦♦	♦♦♦♦	♦♦♦♦	♦♦♦♦	♦♦♦♦	♦♦♦♦
United States	♦♦♦♦	♦♦♦♦	♦♦♦♦	♦♦♦♦	♦♦♦♦	♦♦♦♦
Vietnam	♦	♦	♦	♦	♦	♦
Subnationals	♦	♦	♦	♦	♦	♦

Legend: Sufficient Technologies Capabilities: ♦♦♦♦ exceeds sufficient level ♦♦♦ sufficient level ♦♦ some ♦ limited

Because two or more countries have the same number of diamonds does not mean that their capabilities are the same. An absence of diamonds in countries of concern may indicate an absence of information, not of capability. The absence of a country from this list may indicate an absence of information, not capability.

Figure 2.0-2. Information Systems Foreign Technology Assessment Summary

SECTION 2.1—INFORMATION COMMUNICATIONS

Highlights

- Long-distance, beyond-line-of-sight communications are essential for:
  – Remote reconnaissance and damage assessment,
  – Aerial strikes launched from one country on targets in an adversary country, and
  – Battlefield command and control within large tactical arenas.
- In mixed WMD and conventional conflicts survivable communications are critical to sustaining chemical or biological offensives.

OVERVIEW

The Information Communications Functional Area (FA) as generally defined includes transmission facilities, that is, 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 combine many separate sources of traffic into a single signal to enhance transmission efficiency. In modern designs, transmission termination, switching, multiplexing, and other functions may be integrated in a single piece of equipment and, in combination, play a major role in defining network capacity and latency, communication 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 in the nonintegrated types are simple repeater/amplifiers, channel service units (CSUs), and data service units (DSUs). CSU/DSUs are termination equipment required to connect customer premises equipment (CPE) to telecommunications networks and typically provide transmit and control logic, synchronization, and timing recovery across data circuits.

Other examples include satellite, terrestrial microwave, and cable transmit and receive terminals (transceivers), which, in most instances, include multichannel capabilities. Modern, fourth-generation and beyond switches and digital cross-connect systems (DCSs) incorporate switching, multiplexing and line-termination functions.

In the case of public cellular or specialized mobile radio (SMR) equipment, Information Communications FA capabilities are combined with traditional application-level functions such as call set-up and take-down dialing, signaling, etc.; advanced features like caller identification; and acoustic and other human interface capabilities.

Thus, it is apparent that basic requirements for communicating information between two nodes can be accomplished through the use of a wide variety of COTS products, each with greater or lesser abilities to support WMD operations. Moreover, whether implemented in modern integrated or prior-generation products, Information Communications Functional Area capabilities are critical for WMD missions of any significant complexity or duration.

RATIONALE

Information Communications Functional Area capabilities, including beyond line-of-sight (BLOS) and secure communications, can be important to WMD operational missions and objectives.

Requirements for BLOS communications arise in both strategic and tactical battlefield WMD warfare. 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, there is a need for some form of long-distance communications. Operational situations in which this occurs include aerial strikes launched from one country to targets in another country. Typical targets might be 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 disembark 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, a sophisticated adversary may have a requirement for BLOS communications to relay data from disposable, possibly air-dropped, wide-area, array sensors systems.

Long-distance communications are implemented using terrestrial or satellite relays, long-wave (below 3 MHz) radio transmission, or a combination of these media. Military long-distance systems can be based on either dedicated facilities or shared facilities obtained from public or other common-user networks. Increasingly, modern facilities of either dedicated or shared design, are able to provide integrated voice, data, facsimile, imagery, and video.

At the low-cost end, single-channel long-distance connections can be made today with standard cellular telephones, interconnected to local and long-distance switched networks. In the near future, mobile service from one or more of the following satellite systems—Iridium, Teledesic, Global Star, Odyssey, and Inmarsat—will become available. Tables 2.1-1 and 2.1-2 illustrate pertinent long-distance communications transmission capabilities.

As an example, in the Gulf War, Iraq was unable to sustain its air defense capability after the United States destroyed its air defense communications network. This resulted from direct attacks on communications facilities with conventional, albeit "smart" weapons. WMD conflicts that escalate to nuclear levels impose the possibility of additional "nuclear effects" communications degradation and destruction.

One advantage of chemical or biological warfare is that it does not necessarily threaten physical facilities and infrastructure plants. When employed in combination with conventional or nuclear warfare, many realistic scenarios arise in which the ability to *sustain* any offensive depends critically on survivable communications, which often come under physical attack in mixed conflicts. Under these conditions, home-country communications among various command centers and depots are required to direct long-term WMD assembly and transport to battlefield and/or launch points.

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, equal, though not identical, to International Telecommunications Union (ITU) standards.

As noted above, these systems are expected to be procured for civil use. But, with appropriate Information Exchange switching, multiplexing and digital cross-connect facilities (see Section 2.2), and Information System Management and Control capabilities (see Section 2.5), they can (1) be easily used for military applications and (2) achieve acceptable survivability and robustness in the face of physical attack.

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 shared public network facilities.

These networks not only offer large industry or military customers service indistinguishable from dedicated facilities-based private networks, but deliver those services at lower cost. Moreover, SDNs greatly augment capabilities to modify, optimize, and customize carrier services, in accordance with changing requirements.

Modern commercial telecommunications networks exhibit unparalleled survivability because the market demands it. One of the major U.S. carriers 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. Yet that funnel factor means that to ensure profitability and network availability, one must not concentrate that much traffic without extensive back-up or redundant connections. Fortunately, SDH/SONET standards addressed this problem from the outset.

With automated Management and Control and appropriate switching and multiplexing facilities, SDH/SONET networks can be designed to tolerate massive switch and cable-cut failures. In many instances, service restoration can be virtually automatic—accomplished in 15 milliseconds—a time span short enough to prevent disconnect of existing calls.

For example, dual homing and two or four fiber-based bi-directional line-switched ring (BLSR) diversity among switching/multiplexing hubs, along with designed-in capabilities (like embedded SDH/SONET protection routing and automated performance monitoring and diagnostic management functions), yield survivability features that older dedicated military systems with precedence, priority, preemption, and even dynamic non-hierarchical routing (DNHR) cannot approach.

The explanation for this is that these older techniques basically preserved or restored service on a call-by-call basis. On the other hand, one company has announced its U.S. network plan for 38 interlocking rings, with 16 nodes per ring, that will enable hundreds of thousands of equivalent voice circuits to be restored, almost instantaneously.

Since SDH/SONET systems can accommodate the world's largest common-user network traffic loads, bandwidth or channel capacity requirements encountered in WMD or conventional warfare scenarios can be met without resorting to state-of-the-art switching speeds or ultra-broadband transmission systems.

Satellite-based services offer commercial communications exhibiting significant availability and survivability. One class of service that provides virtually undeniable service is mobile communications via hundreds of satellites through Iridium, Teledesic, and the other systems mentioned earlier. Another class of satellite service supports very small aperture terminals (VSATs) which employ small suitcase-packaged antennas 1.5 to 6 feet in diameter. Finally, high-capacity, multichannel trunk satellite service can be supported with larger but still transportable earth terminals.

Not only is it difficult to electronically jam or physically disable the large numbers of satellites providing such services, but to do so may interrupt service to thousands of worldwide users, whether or not they are involved in a conflict. For practical purposes, satellite-based communications exhibit dual, BLOS and equivalent high-survivability capabilities.

FOREIGN TECHNOLOGY ASSESSMENT

The first column of Figure 2.0-2 contains a comparative representation of foreign technology assessments for the Information Communications Functional Area by country and for subnational groups. All of the developed Western nations in the G8 (Canada, France, Germany, Italy, Japan, Russia, the United States, and the UK), except recently joined Russia, plus the Scandinavian countries, Israel, and Taiwan, have capabilities in all elements of the Information Communications Functional Area, including transmission facilities and required electronic equipment located at nodes along the medium, in their installed base. Of the G8, only Russia has considerable development ahead before she becomes comparable to the other members. However, like China, this comparatively late development may be an advantage to Russia because she is not burdened with a large installed base of outmoded analog equipment and bandwidth-limited non-fiber-optic transmission. Therefore, Russia, China, and other lesser developed countries can more readily expand their capabilities with modern equipment, avoiding performance penalties involved with hybrid facilities. The China assessment may be low since one indicator of China’s Information Communications Functional Area capabilities is that the United States alone takes up 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, and China manufactures its own fiber-optic cable.

Most of the other countries with lesser developed telecommunications (Cuba, the Czech Republic, Egypt, Hungary, India, Iran, Iraq, Libya, North Korea, and Vietnam) have lower Information Communications Functional Area capabilities, which tend to be concentrated around the larger population centers; however, these deficiencies could be corrected in a comparatively short period of time with supplemental satellite systems. For example, Iran’s telecommunications installed base is limited to Tehran and its surrounding area. An exception to this generality is Iraq. Iraq’s baseline telecommunications capabilities are much less concentrated on the population centers and are more country-wide. See subsection 8.11 in Part I of the 1996 MCTL.

Table 2.1-1. Information Communications Technology Parameters

Technology	Sufficient Technology Level	Export Control Reference	Critical Materials	Unique Test, Production, and Inspection Equipment	Unique Software and Parameters
Very-small-aperture terminals (VSATs)	Transport service provided via commercial satellites or via proliferant-owned satellite. Bandwidth sufficient to transmit imagery to mobile stations. Long range, highly available.	CCL EAR 99	None Identified	None Identified	None Identified
Public cellular, local and long-distance exchange, or specialized mobile radio service.	Interference resistant, but limited bandwidth may not support all required traffic types and volume for advanced employment	CCL EAR 99	None Identified	None Identified	Capabilities beyond normal commercial practice.
Long wavelength radio communications	Beyond-line-of-sight (BLOS), greater than 100 m wave-length (below 3 MHz)	CCL EAR 99	None Identified	None identified	Empirically validated code for predicting propagation characteristics of BLOS radio and advanced data encryption for com-pression of algorithms for rapid transfer of data.
Public mobile service via multi-satellite systems, e.g., Iridium and Teledesic, Inmarsat, Odyssey, and Global Star.	Limited bandwidth may not support all required traffic types and volume for advanced employment	CCL EAR 99	None Identified	None Identified	Capabilities beyond normal commercial practice.
Fiber-optic cable installations (See Sections 2.2, 2.5)	Configured to support 2- or 4-wire-based Synchronous Digital Hierarchy (SDH)/ SONET enhanced survivability requirements	WA Cat. 5E, P1; CCL Cat. 5E, P1	None Identified	Specially designed, commercially available fiber-optic cable test equipment.	None Identified

Table 2.1-2. Information Communications Reference Data

Technology	Technical Issues	Military Applications	Alternative Technologies
Very small aperture terminals (VSATs)	Mobile, COTS, mass-produced, low cost (~ $25K). Transport service provided via commercial or proliferant-owned satellite. Satellites subject to jamming and physical attack, but commercial impact may deter attack except under extreme situations.	Long-distance, beyond-line-of-sight (BLOS) communications between target vicinities and C^2I headquarters.	Transport service via proliferant-owned satellite; public cellular, local exchange (LEC) and Inter-exchange (IXC) carriers; public mobile multi-satellite communications, BLOS radio.
Public cellular, local and long-distance exchange, or specialized mobile radio service.	Vulnerability of management and switching centers.	Long-distance, beyond-line-of-sight (BLOS) communications between target vicinities and C^2I headquarters.	VSATs with transport service via commercial or proliferant-owned satellites; public mobile multi-satellite communications; BLOS radio.
Long-wavelength radio communications	Susceptible to jamming and radiometric transmitter position location; limited bandwidth.	Long-distance, beyond-line-of-sight (BLOS) communications between target vicinities and C^2I headquarters.	Public cellular, LECs and IXCs; public mobile multisatellite communications; VSATs via commercial or proliferant-owned satellites.
Public mobile service via multisatellite systems, e.g., Iridium and Teledesic, Inmarsat, Odyssey and Global Star	Service not yet available; multiplicity of satellites decreases vulnerability. Limited mobile channel bandwidth may not support all required traffic and volume types.	Long-distance, beyond-line-of-sight (BLOS) communications between target vicinities and C^2I headquarters.	Public cellular; LECs and IXCs; VSATs via commercial or proliferant-owned satellites; BLOS radio.
Fiber-optic cable installations (See Sections 2.2, 2.5)	SDH/SONET enhanced survivability designs needed to achieve needed availability levels.	Local and long-distance communications for in-country communications.	Metallic or other local and long-distance transmission media.

SECTION 2.2—INFORMATION EXCHANGE

OVERVIEW

Information Exchange (IX) is an IS functional area to which switching and multiplexing are usually assigned. As illustrated in Figure 2.2-1, all forms of circuit, packet, and SDH/SONET transport network-based line and path routing and switching are implied. In circuit switching, the IX functional area encompasses call-by-call [e.g., central office (CO) telephone exchange] as well as channel switching.

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

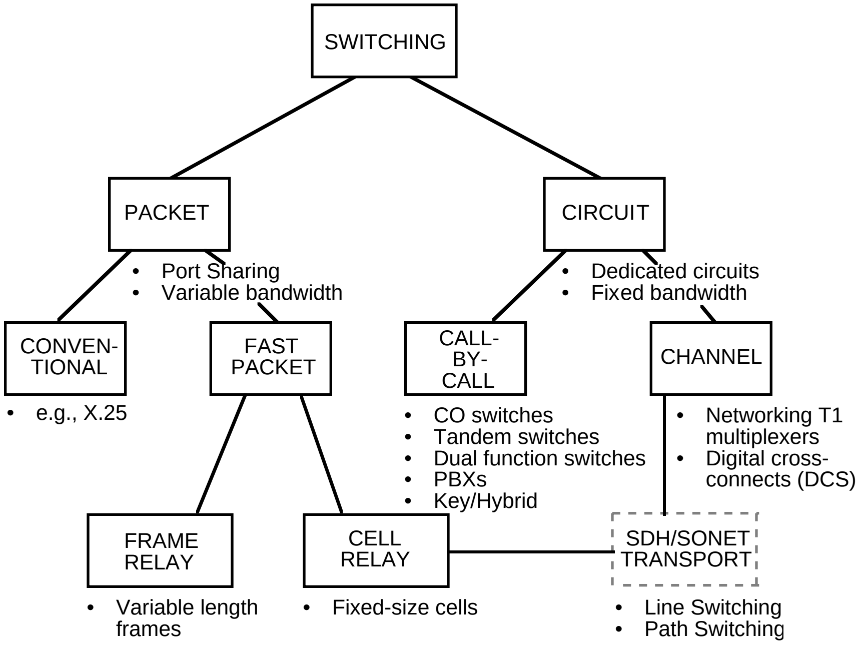

Figure 2.2-1. Routing and Switching Systems

Highlights

- Circuit switching, packet switching, and multiplexing are Information Exchange Functional Area capabilities generally available and installed worldwide, and require constituent elements in all but stand-alone, desktop information systems.
- Stored program control central office and digital cross connect switching are key to Software Defined Networks that can be used for survivable communications capabilities supporting WMD operations.
- Transportable and dual (Central Office and tandem) function switches further enhance network survivability.
- Fast packet, Asynchronous Transfer Mode-based switching and multiplexing support voice, data, graphics, imagery, and video requirements.

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

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

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

Half the available bandwidth in a BLSR is allocated as a working rate evenly distributed among all nodes rather than being funneled through a few hubbing locations, and the other half is reserved for protection routing. Thus, in an optical carrier, OC-48,[1] application, working traffic is placed in the first 24 STS[2]-1 time-slots, with time-slots 25 through 48 serving as the protection facility. In conjunction with ITU Telecommunications Management Network (TMN)-based management functions, this can result in unparalleled recovery from transmission failures, whether 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 DS3 circuits (about 24,000 equivalent DSO (or voice circuits). On July 30, 1996, more than 200,000 circuits were taken out of service when a water department crew bored into a fiber-optic cable in North Carolina. In this case, 92.8 percent of the service was restored in three minutes, nearly 10 times the number of circuits in 3 percent of the time. See Section 2.5 for a discussion of automated Information Systems Management and Control Functional Area technologies that can lead to this kind of performance in networks used to support WMD missions.

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

Another technology category included in the Information Exchange Functional Area is the wide variety of equipment generally described under the rubric of packet switching. As Figure 2.2-1 shows, packet switching encompasses conventional and fast packet realizations in both frame and cell relay appearances. Although it is generally appreciated that modern telecommunications systems are increasingly able to integrate voice, data, video, and other services, as noted earlier an even more systemic form of integration is occurring: that is, the integration of switching and multiplexing within single equipment envelopes.

This development trend is a logical one: early digital circuit switches employed time-division multiplexing techniques (augmented in larger switches with space division multiplexing) to accomplish switching functions.

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[3] (ATM) digital facility. However, more common so-called local area networks (LANs) and satellite access schemes also provide means for sharing common circuits among multiple traffic channels (multiplexing), and provide either connection-oriented or connection-less switching and call establishment functions.

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

RATIONALE

The reason that IX Functional Area capabilities are so important to WMD operations is the same reason that they have commercial significance. Quite simply, IX capabilities are required constituent interconnection elements for any information system that extends beyond a “stand-alone” desktop installation.

Stored program control central office and digital cross-connect switching is key to Software Defined Networks (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 rapidly converted to highly survivable communications assets supporting crucial WMD operations.

Equally valuable for WMD operations is the increased accessibility that end-user organizations have to telephone-company-based SDN management and control facilities that allow them to create and optimize individual subnetworks in accordance with unique customer (in this case, WMD force elements) service and configuration profiles.

In fact, with the exception of long-wave radio, all BLOS and wide-area communications network survivability capabilities described in the Section 2.1, depend critically upon IX capabilities. You don’t build terrestrial or satellite, fixed, cellular, or specialized mobile telecommunications systems 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 all resorted to commercial cellular services for mobile troop communications when military-issue portable radio performance proved unsatisfactory within cities.

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

[2] Synchronous Transport Signal Level 1, basic SONET building block, electrical equivalent of OC-1.

[3] ATM, a cell relay-based form of fast packet switching, uses fixed, 53-byte packets, suitable for voice, data, and other services, in either fixed or variable bit-rate formats.

When operational, Iridium, Teledesic, or other satellite-based capabilities will be even more relevant in satisfying military 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 Information Communications, Information Exchange, and Information Systems Management and Control functional area technologies.

Satellite-based mobile telecommunications of the type just described is one example of commercial technology for which there appears to be no practical military alternative. This statement is true unless one wants to defend the position that there exists in the world a country willing and able to deploy an Iridium or Teledesic-like satellite constellation for dedicated military use only.

COTS dual-function switches that combine central office and tandem switching capabilities are also available. This means that in combination with SDH/SONET transmission systems discussed above, 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 cost-effective means of time-phased upgrading of obsolete telephone systems in urban areas such as Moscow or in many third world metropolitan areas.

Transportable central offices used for disaster recovery by telephone companies represent another commercial technology with significant WMD operations survivability potential. Tables 2.2-1 and 2.2-2 list specific Information Exchange technology capabilities.

FOREIGN TECHNOLOGY ASSESSMENT

The second column of Figure 2.0-2 contains a comparative representation of foreign technology assessments for the IX functional area by country and for subnational groups. The IX functional area capability profiles of most countries are similar to their Information Communications capabilities. There are, however, some exceptions in the cases of smaller or less-developed countries. Iraq's IX functional area is assessed as greater than its Information Communications capabilities, as is Germany's, Japan's, North Korea's, Russia's, and South Africa's, whereas Israel, Poland, and Taiwan are assessed as having fewer IX functional area capabilities than their Information Communications Functional Area capabilities. These lesser IX functional area capabilities can significantly affect the overall performance of their information systems.

The switching and multiplexing capabilities associated with the IX functional area are common to both military and civil systems and have become readily available through joint developments or through foreign sales. The ranking of IX functional area capabilities largely reflects the effects of international standardization. Australia, Canada, Denmark, Finland, France, Germany, Japan, Norway, South Africa, Sweden, Switzerland, and the UK have overall IX functional area capabilities equal to those of the United States, although U.S. capabilities may surpass them in some niche technologies such as optical systems. All of these countries, plus Italy, sell switching equipment worldwide. In most cases, their export equipment is technologically advanced; however, their equipment may incorporate somewhat limited capabilities. For example, their multi-level switching and preemption equipment may contain only two levels rather than three to five levels.

Table 2.2-1. Information Exchange Technology Parameters

Technology	Sufficient Technology Level	Export Control Reference	Critical Materials	Unique Test, Production, and Inspection Equipment	Unique Software and Parameters
International Telecommunications Union (ITU) Synchronous Digital Hierarchy-based/ Synchronous Optical Network (SDH/SONET) switching and multiplexing	Programmable digital byte interleave multiplexers implementing bidirectional line switched rings (BLSRs) providing “reusable bandwidth” in “meshed networks” and protection routing and switching for efficient and self-healing, survivable transmission.	WA Cat. 5E, P1; CCL Cat. 5E, P1	None Identified	Specially designed, commercially available SDH/SONET test equipment	None Identified
Asynchronous digital transmission hierarchy (DS-"n")	Programmable digital cross-connect system (DCS) multiplexers and automated diagnostic management and control.	CCL EAR 99	None Identified	Specially designed, commercially available digital transmission test equipment	None Identified
Conventional and dual-function central office and PBX switching.	Flexible, programmable, tandem, central office, and PBX switching; dynamic non-hierarchical routing, priority and pre-emption.	WA Cat. 5A, P1; CCL Cat. 5A, P1	None Identified	Voice traffic generators	None Identified
Flexible, programmable, variable bit rate-capability, multimedia asynchronous transfer mode (ATM)	Multiplexing and switching for local area network (LAN), metropolitan area and wide-area networks (MAN/WANs).	WA Cat. 5A, P1; CCL Cat. 5A, P1	None Identified	Specially designed, commercially available ATM test equipment	None Identified

Table 2.2-2. Information Exchange Reference Data

Technology	Technical Issues	Military Applications	Alternative Technologies
International Telecommunications Union (ITU) Synchronous Digital Hierarchy-based/Synchronous Optical Network (SDH/SONET) multiplexing and switching	Public capabilities exceed most military requirements. Bandwidth required for WMD is less than commercial networks provide.	Survivable communications among command centers, depots, transportation facilities, industrial centers necessary for WMD operations.	Asynchronous digital transmission hierarchy (DS-"n"). See item below; Public mobile service via multi-satellite systems (see item in Table 2.2-1 above)
Asynchronous digital transmission hierarchy (DS-"n")	Public capabilities exceed most military requirements. Bandwidth required for WMD is less than commercial networks provide.	Survivable communications among command centers, depots, transportation facilities, industrial centers necessary for WMD operations.	An ITU SDH-based broadband transmission system described above; (2) Public mobile service via multi-satellite systems (see item in Table 2.2-1 above)
Conventional, dual-function central office and PBX switching	Requires combined use with synchronous digital hierarchy (SDH) or DS-"n" transmission items to realize benefits.	Survivable communications among command centers, depots, transportation facilities, industrial centers necessary for WMD operations.	SDH and DS-"n" transmission for service restoration
Flexible, programmable, variable bit rate, multimedia for local area network (LAN), metropolitan area and wide-area networks (MAN/WANs)	Public capabilities exceed most military requirements. Bandwidth required for WMD is less than commercial networks provide.	Support for multi-phenomena, wide-area array sensors as they become available; survivability adjuncts to transmission items above.	Less efficient and flexible conventional switching and multiplexing.

SECTION 2.3—INFORMATION PROCESSING

Highlights

- In view of the rapid pace of commercial technology development, the performance of COTS information processing technology is generally far superior to military standard counterparts.
- COTS information-processing design, development, test, and evaluation tools facilitate adaptation and upgrade of older military and commercial information systems, 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

Information Processing (IP) is an IS functional area to which computers, peripherals, servers, end-user or terminal equipment such as displays, keyboards, and other devices are normally assigned. Operating system, application and utility software are also considered elements of the IP functional area. This section discusses many of these technologies, consisting mainly of computer software and hardware.

The following are among an extensive list of IP-based commercial capabilities with WMD application:

- Computer-aided design (CAD) software, hardware suite, and complex system engineering and integration tools;
- A rich variety of IS design, performance and environmental modeling, simulation, test, and evaluation products;
- On-line Analytical Processing (OLAP);
- Streamlined object-oriented programming (reusable programs, classes and objects), fourth-generation languages, and intelligent database management system development/modification products;
- Conventional and advanced multimedia (acoustic, voice, graphics imagery, video, tactile and haptic), user-friendly, human interfaces;
- High-performance virtual reality and other home entertainment products;
- Mature hardware and software products supporting client/server, distributed processing, and database system architectures; and
- Data Warehousing.

In examining the role of commercial technology in WMD applications, it is necessary to understand DoD's overall acquisition policy. Section 2501 of Title 42 of the Defense Appropriations Act for 1993 declares:

> *It is the policy of the Congress that the United States attain its national technology and industrial base objectives through acquisition policy reforms that have the following objectives:*
>
> - *Relying, to the maximum extent practical, upon commercial national technology and industrial base that is required to meet the national security needs of the United States;*
> - *Reducing the reliance of the Department of Defense on technology and industrial base sectors that are economically dependent on Department of Defense business; and*
> - *Reducing Federal Government barriers to the use of commercial products, processes, and standards.*

The implication is that through such policy initiatives, the proliferator seeking to acquire IS can become aware of a wider array of choices.

Just as there is a need to plan for failure or destruction of switching centers in the Information Exchange IS functional area, availability of WMD IP functions ideally must not depend on the survivability of a small number of high-value information-processing centers. Insurance, airline reservation, and other industry segments have developed a wide variety of fail-safe redundancy and back-up technologies, including disaster recovery techniques and plans, that can easily be adopted with great advantage for WMD missions.

RATIONALE

Although COTS capabilities are intrinsically capable of supporting WMD missions, constructing automated strike planing, 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.

However, there is no question that COTS design, development, test, and evaluation technologies outlined above, which are available on the open market, facilitate the adaptation and technology infusion or upgrade of older military and commercial IS, delivery system, and other WMD elements.

Inasmuch as COTS technology transfer to the WMD *Information System* baseline capabilities does not involve composite material, fuel processing, propulsion system, weapon payload integration, and similar structural and mechanical dependencies, much can be accomplished at reasonable levels of effort and within aggressive schedules by rogue countries such as Iran, Iraq, North Korea, and others.

COTS products such as Internet and Intranet capabilities, distributed computing environments (DCE), client-server structures, on-line analytical processing (OLAP), on-line transaction processing (OLTP), an ever-growing family of enterprise software developments, and other commercial developments offer tremendous potential in streamlining and enhancing WMD and conventional warfare operations.

Multimedia personal power-computers are of particular significance for conflict situations in which transportability and information-supported weapons (e.g., remotely piloted vehicles) 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, war-fighting potential even further.

At desktop/workstation capability levels, it is possible today to 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. Tables 2.3-1 and 2.3-2 list specific IP capabilities with WMD relevance.

FOREIGN TECHNOLOGY ASSESSMENT

The third column of Figure 2.0-2 contains a comparative representation of foreign technology assessments for the IP Functional Area by country and for subnational groups. The IP capability profiles of most countries are similar to their Information Communications and Information Exchange capabilities. There are, however, some significant exceptions. India and Iran are assessed as having IP capabilities greater than those in both their Information Communications and Exchange functional areas. Iraq's IP capabilities exceed their Information Systems Management and Control and Information Systems Facilities. Japan, North Korea, and Pakistan have IP capabilities that exceed their Information Communications and Exchange functional areas. Only Australia, South Africa, and Switzerland are assessed as having IP capabilities that are less than their Information Communications and Exchange functional areas.

Some of the country capability assessments that appear in Figure 2.0-2 may be conservative because the IP capabilities in almost all countries are growing so rapidly due, in large part, to the rapid expansion of the Internet. IP technology status statistics by country are difficult to locate; however, some indication of various country's 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 Japan, Germany, the UK, and Canada. Software is changing the economic and military balances in the world. There is an accelerating intellectual capital transfer of software development know-how 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, which teach IP skills and 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 in 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 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.

Table 2.3-1. Information Processing Technology Parameters

Technology	Sufficient Technology Level	Export Control Reference	Critical Materials	Unique Test, Production, and Inspection Equipment	Unique Software and Parameters
Distributed computing environment (DCE), and client-server architectures and structures	Enterprise-wide, compatible information processing functions, preferably with platform independent, WEB/Internet, multimedia plug-in and human interface compatibility.	CCL EAR 99	None Identified	None Identified	Proliferators have the ability to use COTS products in industry-standard applications. Engineering and integration capabilities to adapt COTS products to WMD/ military DCE environments, if not indigenous, are readily available on the open market.
On-line analytical processing (OLAP) and supporting data bases	Using hierarchically organized, n-dimensional databases designed for live *ad hoc* data access and analysis, including consolidation, drill down, vector arithmetic, definable complex variables, time-series data handling, and other capabilities that reduce database size, yield orders-of-magnitude improvement in query response time, and make possible real-time data analyses not possible with conventional designs.	CCL EAR 99	None Identified	None Identified	Proliferators have the ability to use COTS products in industry-standard applications. Engineering and integration capabilities to adapt COTS products to WMD/ military OLAP environments, if not indigenous, are readily available on the open market.
Object oriented technologies (OOTs)	Incorporating class, subclass, inheritance, encapsulation, abstraction and other capabilities such as higher quality software and database products, lower cost and faster development, easier maintenance and upgrade, and reduced lifecycle cost.	CCL EAR 99	None Identified	None identified	Proliferators have the ability to use COTS products in industry-standard applications. Engineering and integration capabilities to adapt COTS products to WMD/ military OOTS environments, if not indigenous, are readily available on the open market.

(cont'd)

Table 2.3-1. Information Processing Technology Parameters (cont'd)

Technology	Sufficient Technology Level	Export Control Reference	Critical Materials	Unique Test Production and Inspection Equipment	Unique Software and Parameters
On-line transaction processing (OLTP) with supporting databases	Supports object-oriented, relational databases and intelligent database management systems to facilitate high volume creation, updating and retrieval of individual records.	CCL EAR 99	None Identified	None Identified	Proliferators have the ability to use COTS products in industry-standard applications. Engineering and integration capabilities to adapt COTS products to WMD/ military OLTP environments, if not indigenous, are readily available on the open market.
"Data Warehousing"	Transforming data into useful and reliable information that supports enterprise decision-making through analytical processing capabilities and applications such as point-in-time data analysis, trend analysis, and data mining.	CCL EAR 99	None Identified	None Identified	Proliferators have the ability to use COTS products in industry-standard applications. Engineering and integration capabilities to adapt COTS products to WMD/ military "data warehousing" environments, if not indigenous, are readily available on the open market.
Data compression and signal processing technologies	Minimizing bandwidth and storage requirements for voice, data, facsimile and other imagery, and video information; implementing optimum matched filter communications components; and enhancing imagery and facilitating pattern recognition and target detection.	CCL EAR 99	None Identified	None Identified	Proliferators have the ability to use COTS products in industry-standard applications. Engineering and integration capabilities to adapt COTS products to WMD/ military data compression and signal processing environments, if not indigenous, are readily available on the open market.
Modeling, prediction, and simulation technologies	Supporting: product design and development; training and evaluation; and enterprise and battlefield planning and decision-making.	CCL EAR 99	None Identified	None Identified	Proliferators have the ability to use COTS products in industry-standard applications.

(cont'd)

Table 2.3-1. Information Processing Technology Parameters (cont'd)

Technology	Sufficient Technology Level	Export Control Reference	Critical Materials	Unique Test Production and Inspection Equipment	Unique Software and Parameters
Computer-based training, distance learning, and group decision support system (GDSS)	Terminal/server/network/teleconferencing technologies incorporating explicit and implicit hypermedia navigation, natural language processing, voice recognition, a variety of "search" engines, an array of person-machine interfaces, and other technologies.	CCL EAR 99	None Identified	None Identified	Proliferators have the ability to use COTS products in industry-standard applications. Engineering and integration capabilities to adapt COTS products to WMD/military GDSS environments, if not indigenous, are readily available on the open market.

Table 2.3-2. Information Processing Reference Data

Technology	Technical Issues	Military Applications	Alternative Technologies
Distributed computing environment (DCE), and client-server architectures and structures	Highly efficient enterprise-wide information-processing functions, preferably with platform independent, WEB/Internet, multimedia plug-in and human interface compatibility; COTS technology exceeds C^2I requirements but modification, adaptation, and extension may be required to support specific military applications.	Enhanced, distributed, survivable intelligence and sensor data fusion, decision support, strike and re-strike planning, strike and damage assessment, micro-meteorological and other modeling and simulation.	Less efficient hardware and software.
On-line analytical processing (OLAP) and supporting databases	Substantial development may be required to adapt military databases and procedures to secure the benefits of this technology.	Military logistic and other warfare planning and decision support. Particularly applicable for strike and re-strike planning, strike and damage assessment, in time-constrained, hot-conflict scenarios.	Less efficient hardware and software.
Object-oriented technologies (OOTs)	Substantial development may be required to adapt military databases and procedures to secure the benefits of this technology.	Enhanced, distributed, survivable C^2I information systems.	Less efficient hardware and software.
On-line transaction processing (OLTP), with supporting databases	Substantial development may be required to adapt military databases and procedures to secure the benefits of this technology.	Military logistic and other warfare planning and decision support. Particularly applicable for strike and re-strike planning, strike and damage assessment, in time-constrained, hot-conflict scenarios.	Less efficient hardware and software.
"Data Warehousing"	Substantial development may be required to adapt military databases and procedures to secure the benefits of this technology.	Military logistic and other warfare planning and decision support. Particularly applicable for strike and re-strike planning, strike and damage assessment, in time-constrained, hot-conflict scenarios.	Less efficient hardware and software.
Data compression and signal processing technologies	Some development may be required to adapt military databases and procedures to secure the benefits of this technology.	Enhanced, distributed, survivable C^2I IS systems	Less efficient hardware and software.
Modeling, prediction, and simulation techniques	Some development may be required to adapt military databases and procedures to secure the benefits of this technology.	Enhanced, distributed, survivable C^2I IS systems and decision-making.	Less efficient hardware and software.
Computer-based training, distance learning, and group decision support system (GDSS)	Some development may be required to adapt military databases and procedures to secure the benefits of this technology.	Enhanced, distributed, survivable C^2I IS systems and decision-making.	Less efficient hardware and software.

SECTION 2.4—INFORMATION SECURITY

OVERVIEW

Technologies in the Information Security (INFOSEC) Functional Area are those designed to safeguard information privacy or secrecy and to ensure information integrity. Encryption, scrambling, protected wire, and steganographic techniques are used to protect the privacy and secrecy of data at or en route among information processing or storage nodes. Hash functions protect information integrity by alerting owners to data manipulation or tampering.

This section deals principally with information in electromagnetic format contained within electronic or photonic devices or en route over suitable media. Physical access control capabilities are included to the extent that they provide protection against attacks intended to illegally acquire information and not merely to physically destroy the facilities in which it resides.

Protecting information while it resides in processing, storage, server, and interface terminal nodes—yet making it readily available to authorized users—is accomplished with access control, authentication, non-repudiation, and electronic signature techniques. All of what has come to be known as "trusted system" INFOSEC capabilities can be used by proliferators.

The cost of trusted systems and other associated COTS INFOSEC products is comparatively small and within the reach of most proliferators. Associated COTS INFOSEC systems that might be used by proliferators for their trusted systems are standard physical and electronic access limiting techniques. Unique badges or cards, which include name, picture, individual personal identification numbers (PINs), other identification numbers, and passwords are in this category. Of Operations Security (OPSEC) interest are advanced local and remote identification and authentication mechanisms. In this latter category are thermogram, hand or eye scanning, voice printing, keyboard rhythm, fingerprint, signature dynamics, and other biometric technologies.

Today there are quality COTS INFOSEC products of such strength that effective communications and signal intelligence countermeasure operations against them are practicable only for government agencies or other large, well-funded organizations. Readily available COTS secure communication products include line and trunk encryption devices, secure voice and data end-instruments, encrypted common channel and per-channel signaling systems, and a rich variety of encryption software.

The availability of powerful and effective INFOSEC products and techniques does not guarantee that any country's computer-dependent enterprise infrastructures are invulnerable. In fact, many of today's computer-dependent utilities such as telecommunications systems and electrical power systems, as well as financial services systems and other civilian and military systems, are known to have been penetrated by competent hackers. Well-funded adversarial government or industrial espionage activities pose an even greater threat to these systems.

Highlights

- Commercial INFOSEC products are available on world markets with capabilities deemed adequate for WMD operations.
- Significant progress is being made toward open, market-based INFOSEC development of public-private key architectures, related standards, and the functional specification of certification authority structures.

Many infrastructure systems are vulnerable, not because they cannot be protected using available COTS products and techniques, but because risk-benefit analyses are not persuasive. Due to their perception of the threat, decision-makers accept the risk rather than bear the attendant investment costs, operating efficiency losses, and time-consuming access restrictions associated with protecting their systems. A knowledgeable proliferator intent on achieving surprise or concealing its identity may be expected to be willing to pay the price of strong INFOSEC.

New and more capable INFOSEC capabilities and techniques continue to appear in both commercial and military environments. And certainly, potential proliferants have ready access to commercial technologies to implement whatever level of security they deem necessary to protect their WMD warfare operations. Commercial technology developments that promise to augment today's capabilities and allow WMD proliferators to implement even higher levels of information security are outlined below.

The use of fiber-optic cable, even in the absence of encryption, greatly complicates the old-fashioned wire-tapping procedure. Intrusion-resistant fiber cable makes undetected eavesdropping almost impossible. Similarly, common-channel signaling defeats automated, in-channel, “search-on-number” intercept techniques, since signaling and subscriber traffic take different signal paths. Proliferants able to use commercial fiber-optic systems would realize these benefits.

Perhaps the most significant open, market-based INFOSEC development is the progress made towards the adoption of public key cryptography and protocols, related standards, and the establishment of certification authority structures. As improved standards and overall architectures emerge, there appears to be more than an adequate supply of scientific and professional competence available for assistance in the development and integration of systems of whatever strength proliferators require, from algorithm and protocol development to encryption and key management.

The financial services industry’s interest and the intense interest of business in electronic commerce on the Internet have accelerated development of commercial tools and technologies with broad WMD application. Among them are means to protect (while selling) intellectual property rights, safeguard databases, restrict access, prevent false repudiation, safely transfer funds, and execute binding contracts electronically, as well as numerous other secure capabilities.

RATIONALE

Because all businessmen and government decision-makers have not implemented measures to correct vulnerabilities in many of today’s nonmilitary systems, the opinion is often advanced that commercial capabilities are unsuited for military applications and their importance to WMD warfighting is minimized. It is unlikely that these arguments will persuade astute WMD proliferators who are free to convert commercial INFOSEC products normally used to protect civilian dual-use information systems to WMD use.

Virtually all commercial INFOSEC capabilities have direct WMD application for weapon storage, custody and release as well as other military command and control operations. In conducting successful nonattributable WMD attacks, covertness is mandatory. In such situations, even the appearance of encrypted traffic may compromise missions by tagging information.

A proliferator may avoid encryption altogether using one-time codes and steganographically concealed messages buried in innocuous text or bitmapped images to prevent adversaries from intercepting intelligible data. This ancient coding method is ideal in high-volume traffic voice and Internet-type data networks. Steganography is within the reach of all proliferators. Even prisoners with no equipment but their minds have developed essentially undetectable means of transmitting embedded decoding templates with the concealed messages.

A complementary approach for maintaining secrecy and covertness involves the use of secure, intrusion-resistant, low probability of detection and interception communications technologies. Of course, if a WMD or conventional attack strategy critically depends on the element of surprise, overt encryption using any of the commercial technologies remains an option.

FOREIGN TECHNOLOGY ASSESSMENT

Complete INFOSEC and OPSEC technical data appears in open source U.S. and foreign trade journals and technical literature and also can be obtained from vendors. Cryptographic systems are widely available. A Russian vendor will deliver a complete package with a 2-year service provision to anyone, and Sun is fielding a whole suite of strong cryptographic products supplied by a Russian manufacturer for their customers anywhere in the world.

National and international export regulations can be circumvented in those countries that prohibit the export of robust information security systems, including strong cryptography. In addition, there are now many countries that have at least a limited capability to produce, or at least use, robust information security products.

The Information Security Functional Area column of Figure 2.0-2 contains a foreign technology assessment by country and for subnational groups. One-third of the countries assessed have capabilities in all INFOSEC Functional Area technologies. Australia, Canada, France, Germany, the UK, and the United States are the world INFOSEC technology leaders. Denmark, Finland, India, Israel, Japan, Norway, Russia, South Korea, Sweden, Switzerland, and Taiwan are close behind the leaders. Iran and North Korea are believed to have all essential INFOSEC functional area capabilities. Most countries and subnational groups, have at least a limited INFOSEC technology capability. A limited capability includes the ability to use INFOSEC products obtained on the world market with little or no direct technical support from the manufacturers. Note that Libya, Vietnam, and the subnationals are among those credited with a limited INFOSEC technology capability and all of them should be able to purchase robust INFOSEC systems, which are comparatively inexpensive.

See Section 2.3 (page II-2-16) for a description of COTS software vulnerability.

Table 2.4-1. Information Security Technology Parameters

Technology	Sufficient Technology Level	Export Control Reference	Critical Materials	Unique Test, Production, and Inspection Equipment	Unique Software and Parameters

Commercial trunk and line encryption system hardware and software	Technologies and products that provide strong link encryption for networks, end-user-to-end-user encryption, and encryption for voice, imagery, video, text, files, and data, all of which could be adapted for C^2I.	WA Cat. 5A, P2;
		CCL Cat. 5A, P2;
		WA ML 11;
		USML XI
			None Identified	None Identified	None Identified

One-time operational codes or commercial software steganographic encoding techniques	Proven COTS products are available for concealing messages in innocuous text or bit-mapped images to transmit covert, low probability of detection and interception politico-military messages. May be used in conjunction with other security measures by any but lowest level proliferant.	WA Cat. 5A, P2;
		CCL Cat. 5A, P2;
		WA ML 11;
		USML XI
			None Identified	None Identified	None Identified

Trusted systems to protect data, processing, and other information systems resources.	Proven COTS products are available which include encryption and hash algorithms, certification authorities, and key management and distribution. Multi-level access control mechanisms including resource segmentation and combined use of unique badges or cards, and local and remote personal identification numbers, passwords, thermogram, hand or eye scanning, voice printing, keyboard rhythm, fingerprint, signature dynamics and other biometric technologies.	WA Cat. 5A, P2;
		CCL Cat. 5A, P2;
		WA ML 11;
		USML XI
			None Identified	None Identified	Pattern recognition algorithms and programs for analysis of biometric features.

Table 2.4-2. Information Security Reference Data

Technology	Technical Issues	Military Applications	Alternative Technologies
Commercial trunk and line encryption system hardware and software	Traffic is susceptible to decryption and spoofing by defending countries with intelligence and information warfare infrastructures. The time scales of WMD operations are typically very short relative to the protection provided by commercial encryption.	Secure C^2I communications for concealing intent during the preparation phase of WMD operations and achieving surprise, controlling force application and obtaining rapid damage assessment in the execution phase of WMD operations.	Wealthy adversaries may choose from a variety of strong COTS technologies and products; poorer adversaries and terrorists may find inexpensive COTS that will provide adequate security.
One-time operational codes or commercial software	Traffic is susceptible to decryption and spoofing by defending countries with intelligence and information warfare infrastructures.	Secure C^2I communications for concealing intent during the planning and preparation phase of WMD operations and achieving surprise, controlling force application and obtaining rapid damage assessment in the execution phase of WMD operations.	None, except for low probability of interception and detection radio transmission techniques.
Trusted systems to protect data, processing and other information systems resources.	COTS equipment exceeds requirements for the WMD planning and preparation phase, but substantial customized modification may be required to provide a secure, end-to-end military system.	Secure C^2I communications for concealing intent during the planning and preparation phase of WMD operations and achieving surprise, controlling force application and obtaining rapid damage assessment in the execution phase of WMD operations.	Less efficient (and less expensive) 3rd generation COTS hardware and software applications are widely available. An alternate to "trusted" systems and products for a minimum WMD capability might be personal recognition and trusted couriers.

SECTION 2.5—INFORMATION SYSTEM MANAGEMENT AND CONTROL

OVERVIEW

Information System Management and Control (IM&C) is the IS Functional Area capability for planning, organizing, designing, optimizing, engineering, implementing, provisioning, monitoring, directing, controlling, and accounting for IS activities and resources. Here, “controlling” is understood to subsume operations, maintenance, configuration and change management, and security. Within the military, IS IM&C is but one element of mission-level Command, Control, and Intelligence functional capabilities. With inadequate IM&C capabilities, a WMD proliferator would have difficulty in rapidly converting civilian telecommunications complex Information Systems to military use or in taking advantage of the survivability Information Systems are able to furnish.

This section addresses IS technologies necessary to control normal operations and service provision while achieving reliability, availability, fault isolation, service restoration, and survivability objectives.

As an example of an advanced IM&C capability, consider today’s software defined or virtual private telecommunications networks (SDN/VPNs), in which traffic is routed through networks under the control of computers residing in network control points or operations centers (NCP/NOCs). These computers are connected to remote stored program-controlled switching and multiplexing equipment using common-channel signaling (CCS) networks. The computers, and associated databases containing a subscriber’s unique VPN information, screen every call and apply call-processing control in accordance with customer-defined requirements.

The IM&C capabilities implemented in an NCP/NOC not only control normal call-processing and routing, but they monitor and manage virtually every aspect of a network. Of particular interest to WMD operations, NOCs are the management and control means by which the extraordinary survivability features of SDH/SONET bidirectional line-switched rings (BLSRs) are realized.

Highly survivable operations, if needed for some WMD missions, can be realized through the combination of fiber-optic and other media Information Communications functional area capabilities; flexible and programmable switching and multiplexing Information Exchange functional area capabilities; and importantly, computer, database, and software IM&C functional area capabilities. Thus, commercial hardware and software product technologies implementing IM&C capabilities can be central to any proliferant’s successful adaptation of commercial public telephone networks for WMD military purposes.

Highlights

- With inadequate Information System Management and Control capabilities, no WMD proliferator can rapidly convert civil telecommunications or other complex IS systems to military use.
- Information Systems Management and Control functional area capabilities are of seminal importance to both normal day-to-day and stressed-mode, complex system operations.
- As information systems grow, add more components, more functions, and more users, IS Management and Control itself becomes more difficult and complex, yet increasingly crucial.

The increasing importance of IM&C to telecommunications and other complex Information Systems is due to many worldwide trends. In the past, data processing was usually accomplished within mainframes in a relatively small number of large, centralized processing sites. In the telecommunications arena, networks supported limited sets of services derived from a relatively small set of basic technologies, using equipment from only a few vendors. Today, divestiture, deregulation, privatization (overseas), and rapid technological expansion and competition has resulted in significant growth in the number of private and public telecommunications networks. These networks support numerous services and are derived from a wide variety of network elements (NEs) with equipment supplied by hundreds of manufacturers.

To cope with added functional complexity and reduce manpower requirements, network operators are placing more processors in voice communications networks (VCNs). Analogously, advances in microprocessors technology and the corresponding trend away from centralized-mainframe designs has spawned a large number of data communications networks (DCNs) now connecting distributed processors in client/server configurations. In both cases, the result is that networks are more complex and more software driven than ever.

Not surprisingly, as information systems proliferate, add more components, more functions and more users, IS management itself becomes more difficult and complex, yet increasingly crucial. The fast growing cellular telephone industry adds new dimensions to telecommunications management, particularly for roaming applications where one carriers' subscribers must be recognized and served by other carrier's networks.

In the United States, divestiture has meant that many end-to-end connections require services and/or facilities from two different local exchange carriers (LECs), one or more interexchange carriers (IXCs) or backbone networks, and often two local area networks comprising customer premises equipment (CPE) from a variety of manufacturers.

Overseas, similar situations exist among interconnected pan-European national networks and within countries where privatization has given rise to a variety of alternative service providers. Effective, integrated IM&C in this environment is difficult to achieve, but may be far simpler in third-world countries, where rebuilding homogeneous nationwide networks from the ground up may be feasible.

Since the IS product environment worldwide is heterogeneous, practical, long-term, and end-to-end (e.g., systems including customer-owned and carrier or other service provider-based, common-user information systems), effective IM&C approaches must be based on standards and a common, evolving agent process/manager process paradigm. Relevant standards include the International Telecommunications Union (ITU), Telecommunications System Sector (TSS) M30X0 Telecommunications Management Network series; the International Standards Organization (ISO) Common Management Information Protocol (CMIP) and several subsidiary standards; the Internet Activities Board, Simple Management Network Protocol (SMNP); and the Institute of Electronics Engineers (IEEE) local and metropolitan area network standard entitled LAN/MAN Management.

To achieve the rapid fault isolation and service restoration leading to ultra-high availability and militarily acceptable levels of survivability, standards must be implemented in appropriate network elements and arranged in architectures with designed-in performance monitoring; fault isolation; and excess traffic, processing, storage capacity, and disaster recovery back-up resources that can be quickly reallocated to compensate for intentional, man-made, or naturally occurring damage or failure.

In public networks, this means stored program central office, tandem and digital cross-connect switching, multiplexing, router and server equipment; telecommunication management networks (TMNs, i.e., data communication networks designed to exchange management information but logically separate from "managed networks"); broadband fiber-optic Synchronous Digital Hierarchy/SONET (SDH/SONET)-based backbone transmission; and alternate multimedia communications (e.g., broadband satellite and satellite or terrestrial based mobile communications). An advanced signaling system such as the ITU-TSS Signaling System # 7 (SS # 7—AT&T and Bellcore versions are commonly referred to as CCS 7 and SS 7, respectively) plays an important role in normal and degraded-mode military operations of advanced telecommunications system. For example, during the Cold War era, COCOM permitted the export of SS # 7-capable switching hardware, but restricted export of SS # 7 itself.

Figure 2.5-1 summarizes IM&C dimensions, i.e., the functions, managed entities, and domains implied in the above discussion. In the figure, IM&C functions are divided into "technical" and "business/government/military" categories, with only key subfunctions illustrated. Managed entities are grouped under "IS Services," "IS Networks," and "IS Elements" categories, again with only partial subcategory illustrations. Finally, the dedicated-facilities and common user management domains are shown.

RATIONALE

Figure 2.5-1 graphically demonstrates the challenges involved in creating either end-to-end integrated management and control systems or achieving the goal of "open IM&C systems." However, as noted, in third-world countries where upgrading essentially allows designers to start with a "clean slate," military information systems can be built upon homogeneous or even single-vendor common-user commercial systems. These systems can easily be more survivable than dedicated, special purpose alternatives built from equipment made to military specifications.

The reason is twofold. First, civil information systems generate revenue only when operational. As a consequence, the profit motivation for high availability, minimum downtime, and immunity to failures and accidental cable cuts is paramount.

Second, although it is possible to design excess capacity into military systems to account for losses in warfare, capacity requirements sufficient to handle peacetime civilian requirements are generally orders of magnitude larger than any justifiable military overbuild design requirements.

To illustrate these advantages, consider the Autovon military network. It was once regarded as the preeminent, survivable voice network with 55 U.S. switch centers. Today civil requirements have resulted in switch numbers and capacities dwarfing old Autovon military requirements. As a consequence, the most survivable military IS designs are those based on the ability to make optimal use of civil systems by placing them at the disposal of military users. This is especially true of commercial technologies embodying the most effective IM&C mechanisms to circumvent outages caused by natural disasters and irreducible component failures. Tables 2.5-1 and 2.5-2 illustrate specific technology capabilities with WMD significance.

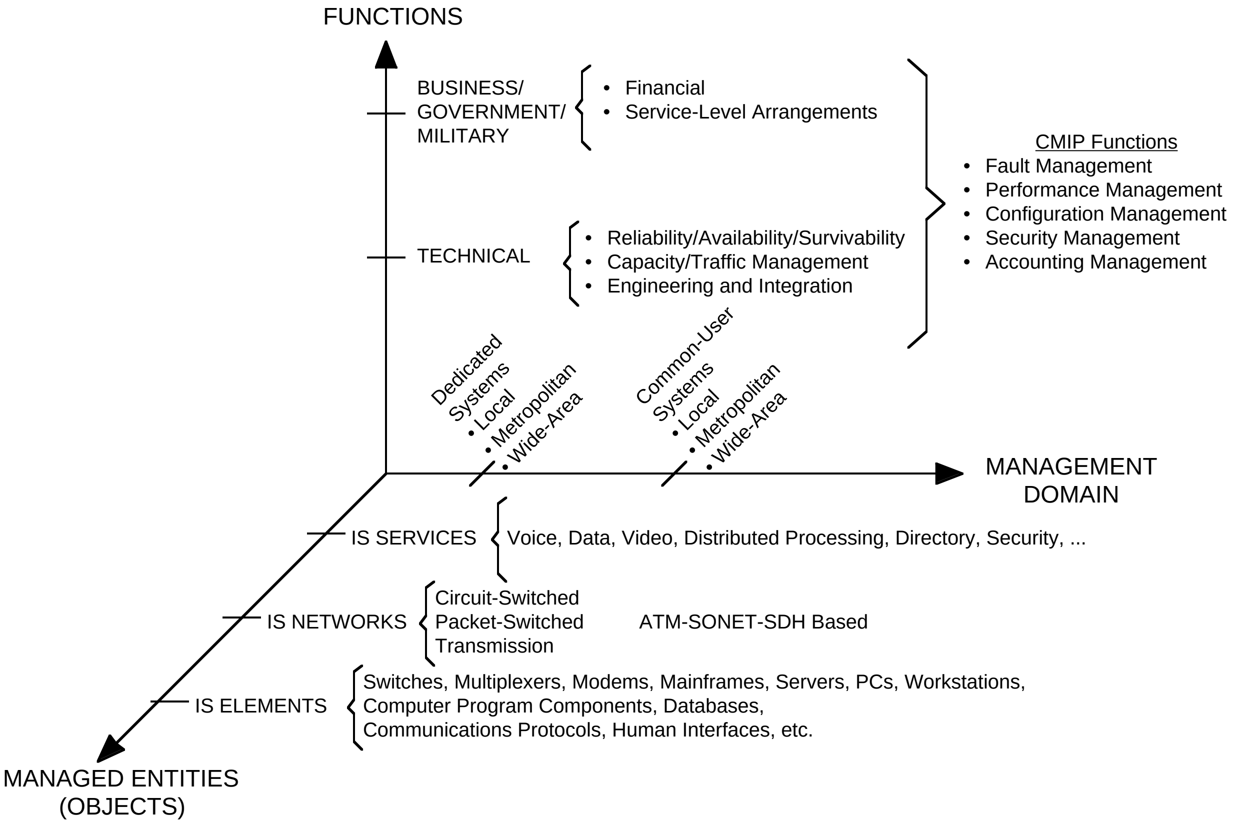

Figure 2.5-1. Information Systems Management and Control

FOREIGN TECHNOLOGY ASSESSMENT

The Information Systems Management and Control (IM&C) column in Figure 2.0-2 shows the comparative IM&C capabilities of 32 countries and a representative assessment for subnational groups. Only one-third of those listed have all IM&C Functional Area capabilities because this is a large, complex, functional area consisting of 11 elements that include the capability for planning, organizing, designing, optimizing, engineering, implementing, provisioning, monitoring, directing, controlling (operations, maintenance, configuration and change management), and accounting for IM&C activities and resources. Countries with strong capabilities in all IM&C technologies are the world Information Systems leaders (or host divisions of multinational companies), which have installed much of the world's information systems telecommunications base. The world's IM&C leaders are Canada, France, the UK, and the United States. In contrast, Iran, Iraq, Libya, North Korea, and the subnationals are among those countries that have only limited, if any, IM&C capabilities. An ambitious WMD proliferator would need strong capabilities in all IM&C technologies to rapidly convert civilian telecommunications and the other complex information systems functional area technologies to military use and take advantage of the extraordinary survivability modern systems could provide for WMD operations. A minimal proliferator that does not intend to conduct sustained or sophisticated WMD operations might not benefit from the possession of IM&C technologies.

Table 2.5-1. Information Systems Management and Control Technology Parameters

Technology	Sufficient Technology Level	Export Control Reference	Critical Materials	Unique Test, Production, and Inspection Equipment	Unique Software and Parameters
Logically and/or physically separate signaling and Telecommunications Management Network (TMN)	Encrypted networks that support normal network operations and service offerings; specially designed to implement real-time management via ATM; dynamic autonomous reconfigurability at all levels of service (intelligent fault recovery); seamless support to broadcast and multilevel, multi-user point-to-point data communications services; hybrid real-time/ non-real-time distributed computing environments incorporating mobile assets; automated data distribution and control from multiple sources. Can monitor and manage virtually every aspect of the network during normal and degraded conditions.	WA Cat. 5A, P2; CCL Cat. 5A, P2	None Identified	Specially designed, commercially available management systems that allow for self test.	Operating systems and network management software incorporating hierarchical, multilevel security; intelligent agents for distributed computing environment monitoring, work load allocation, and dynamic configuration management.
Combined network control point/operations center (NCP/NOC)	Programmable, computer-based facilities for managing and controlling switching, multiplexing, communications, and other network operations.	WA Cat. 5A, P1; CCL Cat. 5A, P1	None Identified	None Identified	Vendor-specific NCP/NOC software
Automated system management system (SMS) hardware and software	Monitors performance, detecting, isolating, and diagnosing failures, rapidly accomplishing restoration and reprovisioning.	CCL EAR 99	None Identified	None Identified	Vendor-specific SMS software

(cont'd)

Table 2.5-1. Information Systems Management and Control Technology Parameters (cont'd)

Technology	Sufficient Technology Level	Export Control Reference	Critical Materials	Unique Test, Production, and Inspection Equipment	Unique Software and Parameters
SMS and network element hardware and software	Implementing evolving TMN and CMIP/SNMP manager process/agent process paradigm-based protocols and object-oriented, management information base (MIB) architectures, models, standards and interfaces.	CCL EAR 99	None Identified	None Identified	Operating system and network management software incorporating hierarchical, multi-level security; intelligent agents for distributed computing environment monitoring, work load allocation, and dynamic configuration management.
Customer or integrated network management systems (CNM/INMS)	Providing end-to-end, global, unified network management of an entire enterprise network.	CCL EAR 99	None Identified	None Identified	Evolving network management software incorporating html/ browser technology
Signaling System (SS) 7	Implementing SS # 7-based encrypted common channel signaling.	WA Cat. 5A, P2; CCL Cat. 5A, P2	None Identified	None Identified	SMS proprietary software to implement SS # 7.

Table 2.5-2. Information Systems Management and Control Reference Data

Technology	Technical Issues	Military Applications	Alternative Technologies
Logically and/or physically separate signaling and Telecommunications Management Network (TMN)	Proprietary products are available within so-called Intelligent Networks but not implemented to the same extent by all commercial telephone companies or PTTs. While the TMN model enjoys nearly universal endorsement, telco carriers and equipment are only making slow progress towards adopting and implementing national or world-wide standards.	Highly efficient, highly survivable, rapidly reconfigurable and reconstitutable C^2I information systems operations.	Earlier generation hardware and software.
Combined network control point/ operations center (NCP/NOC)	Proprietary products are implemented in modern telephone companies and used to render their “flagship” software defined/virtual private network (SDN/ VPN) service offerings.	Highly efficient, highly survivable, rapidly reconfigurable and reconstitutable C^2I information systems operations.	Earlier generation hardware and software.
Automated system management system (SMS) hardware and software	Proprietary products for failure detection and recovery.	Highly efficient, highly survivable, rapidly reconfigurable and reconstitutable C^2I information systems operations.	Earlier generation hardware and software.
SMS and network element hardware and software	Proprietary products are available and used separately in local and long-distance exchange carrier and customer-owned network domains.	Highly efficient, highly survivable, rapidly reconfigurable and reconstitutable C^2I information systems operations.	Earlier generation hardware and software.
Customer or integrated network management systems (CNM/INMS)	Proprietary products are available and used separately in local and long-distance exchange carrier and customer-owned network domains. An SMNP open systems based industry consensus is emerging.	Highly efficient, highly survivable, rapidly reconfigurable and reconstitutable C^2I information systems operations.	Earlier generation hardware and software.
Signaling System 7	None	Highly efficient, highly survivable, rapidly reconfigurable and reconstitutable C^2I information systems operations.	Earlier generation hardware and software.

SECTION 2.6—INFORMATION SYSTEMS FACILITIES

OVERVIEW

Information Systems Facilities is the Functional Area encompassing 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; electromagnetic pulse protection; tempest shielding; radiation protection; and human habitation and life-support accommodations.

Clearly, not all of these capabilities are required for every instance of military operations. Physical shelters may be fixed, or transportable in ground mobile, airborne or shipborne configurations. They may support manned command, control and intelligence centers, manned information processing or communications centers, or unattended IS resources.

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.

Where nuclear weapons are involved, the Cold War era taught that under determined attack, there is no such thing as a survivable, fixed command center or IS operations building. Not even so-called deep underground command centers, regardless of cost, could be certified as survivable. As a consequence, in military WMD scenarios in which long-term survivability is mandatory, mobile facilities are the only viable option. From a U.S. perspective, preparation for global nuclear warfare, beginning with the World-Wide Military Command and Control System (WWMCCS) program in the 1970’s, led to the investment of billions of dollars 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-Tac program developed a wide variety of mobile/transportable voice and data switching, communications satellite and terrestrial terminals, and various IS processing center products to support moving battlefield theater 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.

By the late 1980’s, enormous advances in microprocessor-based computer power, coupled with dramatic reductions in space, weight, and prime power consumption, made possible installation in a single rack those IS capabilities which previously required an 18-wheel tractor-trailer.

Highlights

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

Due to these advances, the trend towards transportable IS facilities accelerated in the 1990’s. 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, and rich varieties of distributed computing environment data processing functions.

Worldwide, many commercial telecommunications carriers inventory central office, tandem, and dual-function switches; cellular/PCS base-station; digital loop carrier (DLC); and other capabilities in transportable/mobile configurations. Alternatively, with broadband, fiber-optic transmission, traffic can be affordability back-hauled great distances to remotely restore damaged or otherwise failed switching, multiplexing, DLC, or other functions.

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

All of the above IS technology capabilities are known to potential WMD proliferants and available on world markets. Thus, the possibility that WMD proliferants will be able to use transportable or mobile IS facilities to mount highly survivable offensives must be fully accounted for in planning by U.S. or allied forces.

RATIONALE

The relevance of older military or commercial, high-technology, highly survivable IS facility capabilities in WMD warfare is evident from the above discussion.

Should a WMD proliferator possess only fixed IS and support facilities, U.S. and allied precision-guided and other conventional weapons can be effective. In future WMD and other conflicts, we may find that adversaries have deployed, or can deploy, transportable or mobile IS facilities. Ominously, in many cases the total cost per transportable IS facility may be an order of magnitude less than the costs 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 WMD users must be fully understood by U.S. strategists and planners if effective countermeasures and counter-strike alternatives are to be available.

See Tables 2.6-1 and 2.6-2 for specific examples of pertinent IS Facility capabilities. Sections 3 (Biological Weapons Technology), 4 (Chemical Weapons Technology), and 5 (Nuclear Weapons Technology) present specific technologies that provide personal and shelter-based protection from chemical, biological and nuclear weapons effects, respectively. Note that survivable IS facilities are not required by proliferators with minimal WMD weapon inventories and capabilities, or those that perhaps would launch isolated WMD attacks.

FOREIGN TECHNOLOGY ASSESSMENT

The last column in Figure 2.0-2 contains a foreign technology assessment by country and for subnational groups in the IS Facilities Functional Area. Countries with advanced Information Systems, and especially those defending against or planning large-scale, sustained WMD operations, need all of the IS Facilities Functional Area capabilities. Only nine of the 32 countries listed have capabilities in all of the technologies in this functional area.

Like the IM&C technologies, the IS Facilities Functional Area technologies are found among the world leaders in Information Systems: Canada, France, Germany, Japan, the UK, and the United States. Denmark, Norway, Russia, and Sweden also have all IS Facilities Functional Area technologies. Several countries have limited IS Facilities Functional Area technologies: Iran, North Korea, and Poland. Iraq, Libya, Vietnam, and the subnationals also have limited capabilities in these technologies.

Proliferants committed to conducting large-scale and sustained WMD warfare need substantial IS Facilities Functional Area capabilities, particularly for operations requiring highly survivable transportable and mobile IS capabilities.

Table 2.6-1. Information Systems Facilities Technology Parameters

Technology	Sufficient Technology Level	Export Control Reference	Critical Materials	Unique Test, Production, and Inspection Equipment	Unique Software and Parameters
Transportable command and force shelters	High mobility and WMD weapon effects protection incorporating closed-cycle or specialized air-decontamination capabilities and radiation-hardened to protect/limit exposure of internal components to a total dose* of 5×10^3 Gy(SI) or a transient dose of 5×10^6 Gy(SI)/sec.	WA ML 13; USML XXI	None Identified	EMI/EMP testing	None Identified
Specially designed tractor-trailer rigs for telecommunications restoration	Equipped with central office and dual function switches, multiplexing and media termination equipment, incorporating closed-cycle or specialized air-decontamination capabilities and radiation-hardened to protect/limit exposure of internal components to a total dose of 5×10^3 (Gy)(SI) or a transient dose of 5×10^6 Gy(SI)/sec, able to restore transmission and call center service and rapidly deployable via road, rail, or air shipment.	WA ML 13; USML VII	None Identified	None Identified	None Identified
Transportable base stations	Provides and with the ability to rapidly deploy or restore terrestrial cellular, PCS, or SMR service. Incorporating closed-cycle or specialized air-decontamination capabilities and radiation-hardened to protect/limit exposure of internal components to a total dose of 5×10^3 Gy(SI) or a transient dose of 5×10^6 Gy(SI)/sec.	WA ML 13; USML XXI	None Identified	None Identified	None Identified

* The dose rates are expressed in *Système Internationale d'Unités* (SI) metric units of radiation. The gray (Gy) is a unit of absorbed dose of ionizing radiation; one Gy is an absorbed dose of ionizing radiation equal to one joule per kilogram of absorber. The gray replaces the rad. One rad = 0.01 Gy.

Table 2.6-2. Information Systems Facilities Reference Data

Technology	Technical Issues	Military Applications	Alternative Technologies
Transportable command and force shelters	Degree of ability to withstand bombs, missiles, or WMD weapons effects	Highly survivable C^2I and trans-attack conflict execution operations	Use other fixed and mobile assets as available
Specially designed tractor-trailer rigs for telecommunications restoration	Deployment and activation rates under military conflict situations	Highly survivable switching, multiplexing and multimedia communications capabilities	Use other fixed and mobile assets as available
Transportable base stations	Requires combined use with survivable wireline telco service items to reap maximum benefits	Survivable home-country and theater of operations communications (see additional citations above)	Use other fixed and mobile assets as available