

# Chapter 9

## Information Assurance for the Tactical Environment

---

Communicating urgent, time-sensitive, or life-and-death information over wireless links in a military or quasi-military tactical environment presents unique information assurance (IA) challenges. This section addresses the specific security concerns associated with tactical information systems, and points out critical technology gaps in today's tactical communications environment. The section highlights key tactical-specific issues in an effort to generate credible IA criteria, resulting in a significant and positive impact on IA technology developed by industry.

The first part of this section focuses on a description of the tactical environment and the types of threats specific to this environment. The latter part of this section covers several IA issues facing tactical users. Current and anticipated requirements for IA solutions are drawn from these issues. Finally, each section identifies current technologies in development or production that may satisfy key IA requirements, provides framework guidance on recommended technologies, and identifies substantive gaps in available security solutions. This insight will help guide United States (U.S.) industry in developing security technologies to satisfy the needs of tactical users. It also will assist government users in understanding the range of security solutions available and the manner in which these solutions might be used.

Although some of the key technologies discussed here may have been mentioned in previous sections of the Information Assurance Technical Framework (IATF), the unique requirements of the tactical environment warrant a separate discussion for the benefit of equipment developers, integrators, and warfighters. This section focuses exclusively on those issues in which the tactical environment presents unique requirements for IA technologies. Tactical users should refer to other sections of this IATF for guidance on common IA technologies such as firewalls, virtual private networks (VPN), and intrusion detection systems.

This chapter of the IATF will be useful to the following types of organizations.

- U.S. Department of Defense (DoD) and commercial engineering support organizations responsible for design, integration, and life cycle support of tactical communications and information processing equipment.
- Military and other DoD organizations involved in conducting tactical operations.
- Other nonmilitary organizations involved in tactical operations (e.g., law enforcement; Alcohol, Tobacco, and Firearms [ATF]; Drug Enforcement Agency [DEA]; the Coast Guard; emergency responders; search and rescue units; Immigration and Naturalization Service [INS]; and other agencies involved with National Security and Emergency Preparedness [NS/EP] communications).

- Anyone whose operations are mobile or who has heavy reliance on urgent, time sensitive, or life-and-death information often communicated over radio frequency (RF) links.

## 9.1 Target Environment

### Definition of Tactical

In this context, tactical communications refers to a set of systems, products, and infrastructure that transfer time- and content-sensitive communications between wireless nodes, or from wired to radio transmission environments. These systems are used typically in military-style operations and require specific frequency allocation and spectrum management to avoid electromagnetic interference with commercial and civil communications.

The following set of characteristics is used to define tactical.

- Military-style operations.
- User-owned (or leased) equipment and infrastructure.
- Radio communications in licensed frequency bands.
- Communications in a hostile physical and RF environment.
- Classified or Unclassified but Controlled communications.
- Time-sensitive communications.

Because of the unique nature of the tactical environment, certain types of attacks are more common than others. Previous sections of this framework divide attacks into four categories: passive, active, insider, and physical and distribution. Tactical forces place a high degree of trust in individual unit members and in the communications systems available for their mission. However, as the information transport network in tactical environments is often RF based, the potential still exists for an adversary to gain access to internal tactical communications systems, masquerading as an authorized user. The adversary then has the potential to conduct an insider attack. Thus, tactical communications systems must also defend against these types of attacks.

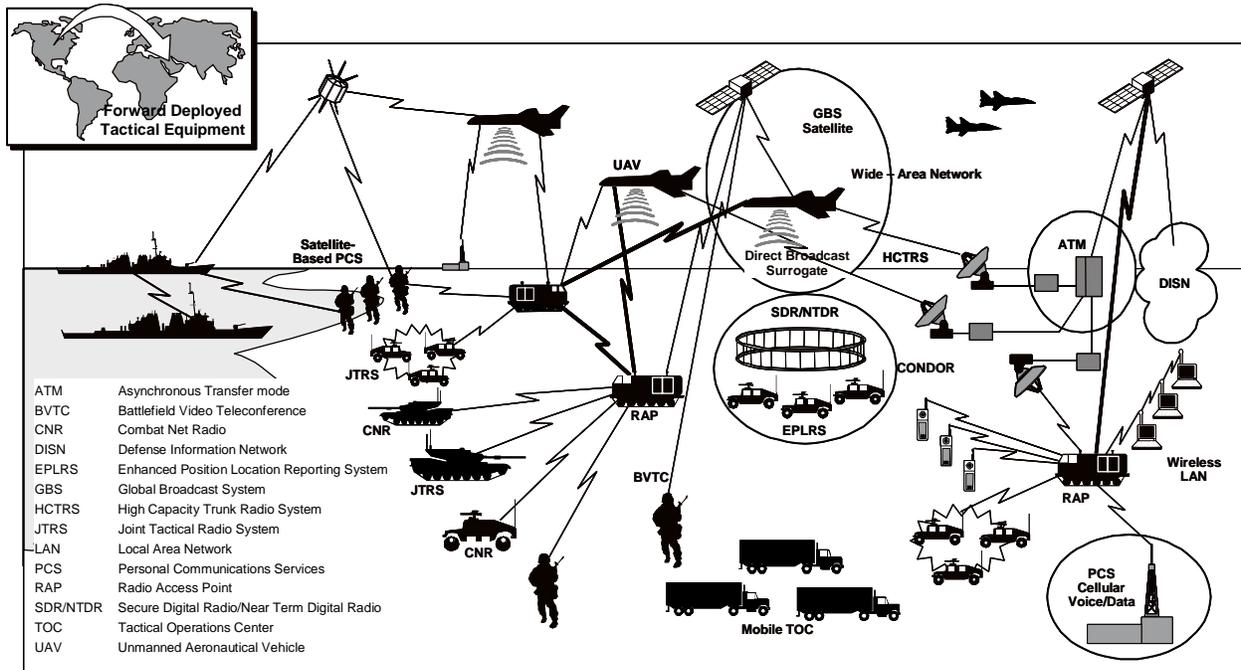
A majority of tactical communications systems are subject to both passive and network attacks by highly sophisticated adversaries, often with abundant resources. Although not a tactical site attack, the recent Kosovo conflict demonstrated an increase in the sophistication of our adversaries. Individuals sympathetic to the Serbian forces attacked several U.S. and North Atlantic Treaty Organization (NATO) Web sites. Although most of these were denial of service attacks against publicly accessible Web pages, more complex and malicious attacks can be anticipated in future conflicts.

As noted in Section 5.2, Wireless Networks Security Framework, commercial wireless users and service providers are often concerned with theft of service attacks. However, tactical users of wireless communications systems are concerned with more destructive attacks threatening lives, or the national security, or both. Specific attacks that many tactical users want to prevent are as follows:

- Geo-location (determining location of operators, confidentiality).
- Detection and interception of communications traffic (confidentiality).
- Jamming communications traffic (denial of service).
- Communications traffic analysis (gathering knowledge of activities from patterns of communications usage).
- Network intrusion and associated masquerading attacks (integrity, false message insertion, and password sniffing).
- Theft of sensitive/classified information (confidentiality).
- RF fingerprinting (association of a particular medium with a specific user; i.e. unit identification based on radio characteristics).

## Military Examples

Examples of tactical communications scenarios vary based on the specific missions and military services involved. Figure 9-1 illustrates the complexity of deploying a total-force tactical communications suite to a battlefield. The figure also shows the warfighter’s reliance on key access points (satellite links and Unmanned Aerial Vehicle [UAV] airborne communication nodes) used to access the larger communications infrastructure. Communications architectures for nonmilitary tactical operations can have similar characteristics.

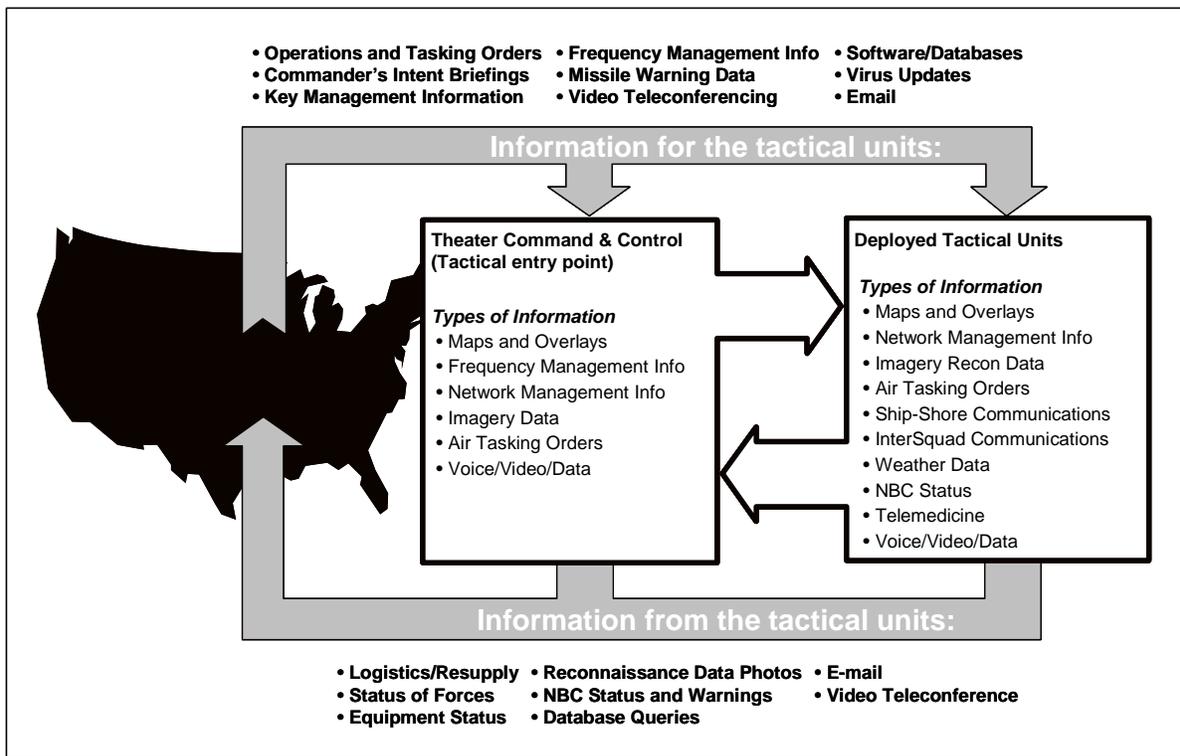


iatf\_9\_1\_0129

Figure 9-1. Tactical Communications Environment

Clearly, not all of the systems shown in Figure 9-1 are interoperable, as the figure might suggest. A majority of current tactical communications have a low degree of interoperability among the military services. However, future systems like the Joint Tactical Radio System (JTRS) will provide increased interoperability among the military services' and allied networks, yielding an increased command and control (C<sup>2</sup>) capability for decision makers.

Figure 9-2 shows the types of information flowing into and out of a typical tactical environment to U.S. command sites. Major operational functions such as frequency management are often handled at a Main Operating Base (MOB) or command center, rather than on the front lines. Other functions provided from Continental U.S. (CONUS) locations include missile warning information from the North American Aerospace Defense (NORAD) Command, and nuclear, biological, and chemical (NBC) fallout tracking from Los Alamos National Lab. These types of information pass back and forth between tactical forces and fixed locations in CONUS. Additionally, critical databases and imagery information are maintained either at the MOB or at the theater headquarters. Tactical units can access information on an as-needed basis, instead of bringing extra equipment to the front lines. Thus, a vast amount of data flows continuously between the main base in CONUS, the forward base, and forces on the front lines in a tactical scenario.



iatf\_9\_2\_0130

Figure 9-2. Tactical Communications Information Flow

Tactical communications are often defined by their environment and purpose rather than the specific equipment in use. In the past, tactical communications equipment was primarily composed of government off-the-shelf (GOTS) equipment. Such unique or "closed" systems,

however, often require extensive support throughout their life cycles. In addition, it is often not cost effective to try to expand their capabilities to meet new requirements. Even with increased government budgets, the need for more capability has outstripped resources. Increased interoperability requirements and faster technological evolution have resulted in the increased use of commercially developed equipment in tactical communications. The trend in today's tactical equipment design is to build open architectures where new advances can be added to systems efficiently.

A key example of DoD movement toward an open architecture is the JTRS. Recently, DoD identified the needs and benefits of combining various radio acquisition programs being proposed by the Services. As a result, DoD proposed the development of a family of affordable, high-capacity tactical radios to provide line-of-sight (LOS) and beyond-line-of-sight Command, Control, Communications, Computer, and Intelligence (C4I) capabilities to warfighters. This family of radios will be capable of covering an operating spectrum from 2 to 2000 Megahertz (MHz) and will be capable of transmitting voice, video, and data. However, the JTRS is not a "one-size-fits-all" solution. Rather, it is a *family* of radios that is interoperable, affordable, and scalable. By building on a common architecture, JTRS will improve interoperability by providing an ability to share waveform software and other design features between radios. The goal is to migrate today's legacy systems to systems compliant with the JTRS architecture. Section 9.8.3, Technology Assessment presents a more in-depth discussion of the JTRS.

The challenge of moving to an open architecture while remaining backward compatible with existing legacy equipment and systems can seem overwhelming. Military systems have traditionally been designed for a specific type of environment, with little regard to future universal interoperability. However, tactical communications systems in the future will be required to interoperate effectively. For example, until recently, two separate devices were required if a commander wanted to place a call on a local cellular system and on a satellite communications (SATCOM) link. Today, a single telephone will operate on both standard cellular and low-earth orbit (LEO) satellite systems. Ideally, this same cell phone can then be integrated into other tactical communications networks like the Mobile Subscriber Equipment (MSE)/Tactical Packet Network (TPN) suite of equipment to maximize the operator's connectivity in the tactical environment, while minimizing the volume of equipment carried. To realize this vision, tactical systems will need to support common signaling plans and protocols such as Internet Protocol (IP) and Future Narrow Band Digital Terminal (FNBDT). Additionally, future systems such as the JTRS will handle multiple frequencies, multiple types of data (voice, data, and video), and multiple waveforms. Warfighters will drastically improve their situation awareness by accessing vital intelligence databases and imagery. Future tactical cellular systems and personal digital assistants (PDA) will allow troops to pull down current satellite images or update enemy locations on the commander's map, giving the commander a better picture of the battlefield. However, these information advantages can be only realized, if the tactical information and communications systems possess sufficient levels of IA.

## Civilian Examples

Nonmilitary organizations also employ systems that meet the tactical communications definition presented earlier. Examples are as follows:

## UNCLASSIFIED

Information Assurance for the Tactical Environment  
IATF Release 3.1—September 2002

- First responders deploying to a terrorist incident.
- Communications support to the Secretary of State during travels.
- Civil departments and agencies deploying to support missions under a variety of operational plans.
- Industry deploying network disaster recovery teams, cellular sites on wheels, and satellite telephone banks into disaster areas, as was the case in 1995 during the Hurricane Marilyn response on St. Thomas, VI.

A particularly interesting example is the new Florida Veterans Mobile Service Center consisting of a 43-foot mobile medical/dental clinic and veterans benefits. The center uses four cellular phone connections, two satellite links, and two laptop computers to link counselors with the state's Department of Veterans Affairs (VA) medical centers and benefits office, allowing them to access veterans' records and medical histories. Videoconferencing equipment allows VA physicians to interview patients directly from the mobile unit.

Probably the best example of nonmilitary tactical operations is the Federal Emergency Management Agency (FEMA) in its role under the Federal Response Plan (FRP) as the coordinator of federal responses to Presidentially declared disasters and emergencies. FEMA coordinates FRP consequence management support to numerous national plans, including the Federal Radiological Emergency Response Plan, the National Oil and Hazardous Substances Pollution Contingency Plan, and the Federal Bureau of Investigation's (FBI) Weapons of Mass Destruction Incident Contingency Plan.

As consequence manager, FEMA is responsible for organizing federal efforts to protect public health and safety, restore essential government services, and provide emergency relief to minimize the effects on the populace of a natural, technological, or terrorist event. To support the various operational facilities and teams that respond in accordance with the FRP, FEMA can deploy telecommunications assets from its six Mobile Emergency Response Support (MERS) detachments located in Massachusetts, Georgia, Texas, Colorado, and Washington and its Mobile Air Transportable Telecommunications System (MATTS) located in Virginia.

MERS and MATTS assets can deploy to a disaster area to support federal, state, and local responders using a variety of communications transmission systems such as satellite, high-frequency, and microwave LOS interconnected by fiber optic cables to voice and data switches, local area networks (LAN), and desktop devices such as personal computers and telephones. Telecommunications can be provided for single or multiple locations within a disaster location. MERS and MATTS telecommunications assets can establish or reestablish communications connectivity with the public telecommunications system or government telecommunications networks and can interconnect facilities within the disaster region.

MERS and MATTS include these telecommunications transmission capabilities:

- Satellite. Ku-band satellite for quick connectivity that provides up to 48 lines for either telephones or data. International Maritime Satellite (INMARSAT) and American Mobile

Satellite Corporation (AMSC) satellite terminals provide immediate single voice channel capabilities.

- LOS Microwave. Microwave transmission to connect to the public network (PN), provide connection to other facilities, or extend communications.
- High frequency (HF) radio to communicate with federal, state, and local emergency centers via the FEMA National Radio Network and FEMA Regional Radio Network.
- Very high frequency (VHF) and ultra high frequency (UHF) radio for local communications.

When deploying in a possible tactical situation, nonmilitary organizations face some of the same IA issues and requirements as DoD. The requirements most important to nonmilitary organizations are interoperability among response elements and protection from the following:

- Interception of communications traffic that is normally unclassified but may be sensitive.
- Denial of service.
- Network intrusion.

## **Layout of the Tactical Communications Section**

To adequately scope the key IA issues facing U.S. tactical forces today, representatives from the tactical community contributed to a list of the leading IA issues to be discussed in this section of the IATF. This list is certainly not all encompassing and may vary in order of importance for different users. However, the issues discussed here will apply to a variety of users and will highlight the IA deficiencies that exist in current systems. Joint and service-specific documents such as Joint Vision 2010 and the U.S. Army Warfighter Information Network document are used as key reference points for many of the tactical issues and requirements discussed in this section of the Framework. Unless otherwise noted, these issues are consistent with the issues described in the Service's forward-looking documents.

The following key IA issues identified by the tactical community are discussed in this section:

- Wiping Classified Data From Tactical Equipment (9.2).
- Stored Data Protection in a Hostile Environment (9.3).
- Key Management in a Tactical Environment (9.4).
- Network Mobility/Dynamic Networks (9.5).
- Access to Individual Classified Accounts by Multiple Users (9.6).
- Secure Net Broadcast and Multicast (9.7).
- IA Solutions in Low Bandwidth Communications (9.8).
- Split-Base Operations (9.9).
- Multilevel Security (MLS) (9.10).
- Additional Technologies (9.11).

## UNCLASSIFIED

Information Assurance for the Tactical Environment  
IATF Release 3.1—September 2002

Within each topic area, a brief overview is provided, followed by a discussion of IA requirements related to each topic. Tactical communications system users have critical equipment and infrastructure requirements beyond what the typical civil or commercial user requires. Anticipated requirements are added in the discussion to highlight requirement areas that will likely need to be addressed for tactical forces five to ten years in the future. These anticipated requirements are based on forward-looking documents such as Joint Vision 2010, the Concept for Future Joint Operations, and the Warfighter Information Network (WIN) Master Plan.

Note that these anticipated requirements should not be considered essential for operations in a tactical scenario. Clearly, warfighters today employ technologies that do not meet many or all of these requirements. Rather, new technologies that incorporate these requirements would be better suited for tactical use than current systems. Thus, development of such technologies will improve the IA inherent in future tactical equipment and systems.

After the requirements discussion, relevant current technologies are addressed. Finally, each topic concludes with a section regarding Framework guidance. The guidance section presents technology recommendations for tactical users and Information System Security Engineers (ISSE), and technology gaps highlight areas for future industry developments.

## 9.2 Wiping Classified Data From Tactical Equipment

### 9.2.1 Mission Need

U.S. military forces have been involved in an increasing number of nontraditional operations in recent years. Joint and multinational operations, peacekeeping missions, and support of FEMA efforts present challenges to the security of U.S. forces and systems that never before existed. During the same period, the U.S. military has adopted a host of new information and communications capabilities. Equipment formally used at the secret or NOFORN levels also is used for unclassified FEMA operations and in multinational operations. In recent years, nation states that were once on opposite sides of conflicts are now part of the NATO coalition forces. Thus, a new requirement has emerged to reuse tactical communications equipment at different classification levels for a variety of missions. IA technologies must be employed to provide a high degree of assurance that sensitive information used in one mission is completely wiped from the equipment before it is used in subsequent missions.

Tactical data wiping is typically performed for one of three primary purposes: equipment storage, national level reuse, or multinational reuse. Residual classified or other sensitive information must be totally erased from any storage media residing in tactical communications or computer equipment. This includes information at several different classifications and handling caveats. The reuse of tactical communications equipment at different classifications

## UNCLASSIFIED

Information Assurance for the Tactical Environment  
IATF Release 3.1—September 2002

applies to most types of equipment. In the past, systems such as the Secure Telephone Unit Third Generation (STU)-III solved this problem by implementing a Crypto-ignition Key (CIK) for each STU-III. The combination of a STU/CIK can be programmed to operate at any classification level. When the phone and the key are separated, they are each considered an Unclassified/Controlled Communications Security (COMSEC) Item (CCI). Similar technologies are used in TACLANE and FASTLANE encryptors, as well as with the Krypton Personal Computer (PC) card in the tactical Secure Telephone Equipment (STE). However, creating these keys can take up to a week. Future use of programmable cryptography, multilevel security solutions (see Section 9.10.), and over-the-air updates for Type 1 cryptography will help alleviate this issue.<sup>1</sup>

For many years, tactical forces used communications equipment in a system-high environment. In other words, if the system handled information up to the secret level, all equipment on the network was treated as secret. Units often purchased multiple systems to operate at different system-high classification levels. In some cases, declassification of equipment for reuse in another situation was possible, but time consuming. Declassifying equipment for use at lower classification levels will continue to take weeks, if not longer. When declassification is done before putting equipment into storage, the tactical user may be able to afford the extra time. However, if the equipment will be reused nationally or internationally, time may be a critical factor. In some cases, the declassification process may be overlooked entirely because of urgent mission requirements. With today's limited budgets, U.S. forces do not have the luxury of purchasing multiple sets of systems for each level of classification. Furthermore, the number of multinational operations in which U.S. tactical forces are involved has increased dramatically and will continue to increase in the coming years. Thus, finding solutions for this issue is vital. If IA solutions are not in place to enable rapid equipment reuse at different classification levels, tactical forces will be forced to purchase additional equipment for each system-high level or accept the risk that sensitive information will be compromised. The interim solutions of purchasing additional sets of equipment and relying on a time-consuming declassification process must be replaced by faster, higher assurance solutions.

As an example of multinational reuse of tactical equipment, recent NATO operations in the Balkans and U.S. operations in Afghanistan have demonstrated the trend toward use of multinational forces in tactical operations. U.S. forces frequently report to coalition commanders from other nations. In addition to the usual issues (language, standard operating procedures) arising from a multinational chain of command, U.S. forces must protect cryptographic keys and algorithms from falling into the wrong hands because a coalition partner today may be an adversary tomorrow. To prevent our IA solutions from being used against U.S. forces in the future, security solutions such as tamper-proof cryptography, programmable cryptographic chips,

---

<sup>1</sup> Throughout this chapter (and other chapters and sections), reference is made to Type 1 strength cryptography. In traditional usage, this has meant government-developed or -sponsored equipment containing security mechanisms that meet some minimum strength of implementation. Enough assurance mechanisms were in place to reduce compromising failures to acceptable levels. In the context that the term is used here, Type 1 is generalized to include any source of equipment provided that robust minimums of cryptographic strength and assurance mechanisms have been included in the design. The exact definition of these assurances and strengths is beyond the scope of this document. This definition of Type 1 is also used in Section 5 (Defend the Network and Infrastructure).

and over-the-air key load and zeroize functions should be implemented in future tactical communications equipment.

## 9.2.2 Consolidated Requirements

- IA technologies must be available to completely remove sensitive information from storage media on tactical communications and computer equipment and ensure that the data is not recoverable.
- IA technologies must allow for equipment reuse at different classification levels.
- Equipment declassification processes must be accomplished rapidly (in a matter of minutes).
- Solutions such as tamper-proof cryptography, programmable cryptographic chips, and over-the-air key load and zeroize functions should be implemented in future tactical communications equipment.

## 9.2.3 Technology Assessment

To prevent our IA solutions from being used against U.S. forces in the future, security solutions such as tamper-proof cryptography, programmable cryptographic chips, and over-the-air key load and zeroize functions should continue to be implemented in future tactical communications equipment. A viable multilevel security solution, discussed in Section 9.10, Multilevel Security (MLS), also may help address this issue.

For computer hard drives and other magnetic media, several software packages exist to purge classified data from a storage device. Two primary types of wiping software are available today: software that purges all data from a media, and software that purges deleted data from a media. These packages also can be used by certain tactical units to purge data from PCs and other magnetic media. However, much of the legacy communications equipment used by tactical units does not interface well with PC software or PC-based networks. Tactical radios may store sensitive information about a particular communications network that has to be erased before reusing the equipment in an unclassified scenario. Legacy cryptographic equipment can usually be zeroized with the press of a button, and new keys can be loaded at different classification levels. However, many of these legacy cryptographic systems are still considered sensitive even after they have been zeroized because of their internal design and the algorithms used. Newer programmable cryptographic chips will be able to wipe keys and algorithms from the chip, leaving a totally unclassified chip capable of being reloaded with new keys and algorithms.

With standard workstations, the weaknesses of current operating systems (OS) make the reuse of computers for different classification levels especially vexing. The allocation of data in swap files, the creation of temporary files, the storage of data in slack and unallocated space, and the actual nondeletion of data despite using the delete command all constitute a potentially serious security hazard. Given the easy availability of hacking tools and forensic software, the

possibility of data recovery is especially high. Although commercial off-the-shelf (COTS) memory shredding application software (e.g., BC Wipe, Erase, Kremlin, and Puffer) exists—and there is a DoD standard for file wiping—the most secure solution is the total removal of all previously used storage media prior to reuse of the basic computer. This decision should be based on a careful risk analysis of the individual situation.

**Note:** Users should consult local security policy for a list of approved wiping software before using any of the software applications listed above.

## 9.2.4 Framework Guidance

Given the current state of technology, the best available solution continues to be removable storage media and zeroize functionality. Equipment can easily be reused in different missions by inserting a new storage media at the appropriate classification level. The zeroize function would also allow new cryptographic keys to be loaded at the appropriate classification level for the new mission. The desired solution involves the use of programmable cryptographic chips used in conjunction with a secure OS. The secure OS ensures that all copies of sensitive files are handled at the appropriate classification level. Users without the appropriate authorizations cannot access the protected information. The programmable cryptographic chip would allow simple key and algorithm updates capable of upgrading or downgrading the equipment classification. Development and use of both programmable cryptography and secure OS are in their infancy. As technology matures, new solutions will be available to address this issue.

## 9.3 Stored Data Protection in a Hostile Environment

Tactical forces always have been faced with the possibility of enemy capture or overrun and the seizure of critical, sensitive, or classified information. In modern warfare, an increasing amount of information is stored electronically. Although this has reduced the volume of sensitive documents and cryptographic material that must accompany a tactical unit to the battlefield, the problem of quickly destroying classified information in an overrun situation has merely changed—not been eliminated. Implementing strong, high-speed, and high-volume media encryption technologies would help mitigate the danger of compromised information, even if tactical communications or information system equipment falls into enemy hands. Alternatively, robust means of quickly rendering digital media unreadable are necessary.

The tactical requirement for media encryption differs from a nontactical situation in two primary areas. First, the information stored in tactical equipment is often very perishable or time sensitive. That is, after a period of time, the utility of the information expires and it no longer requires protection. Although this is not true for all tactical data, typically the media encryption needs to be only good enough to prevent the enemy from breaking the encryption within a short period (days to weeks). For example, information concerning an upcoming attack is classified

## UNCLASSIFIED

Information Assurance for the Tactical Environment  
IATF Release 3.1—September 2002

only before the attack takes place. If information stored on a system pertains to an attack happening in three days, the encryption may only need to be strong enough to prevent an adversary from accessing the information for a week or more.

Second, tactical users often require extremely fast (near real time) media encryption. The media encryption process should be transparent to the tactical user, allowing the user to control the process in real-time and quickly protect the information in a time of crisis. If an Army unit is under attack by the enemy, a soldier may require the capability to rapidly encrypt large storage devices in case the enemy captures the equipment.

### 9.3.1 Mission Need

Equipment subject to theft or recovery by an adversary must have the capability to adequately protect the information stored within the equipment. Current media and file encryption techniques are too slow for use in tactical situations. Media encryption of 1 to 2 GByte hard drives must be accomplished within minutes rather than hours. In tactical situations, zeroization is often used to destroy sensitive information if enemy forces will likely recover the equipment. Until strong, fast media encryption technologies are developed, zeroization will continue to be used in these situations. Once the equipment is zeroized, critical data is lost forever, and it cannot be recovered if the equipment is not captured. Thus, soldiers are often hesitant to hit the zeroize key if there is a chance of defeating the attackers. Unfortunately, this sometimes means that capture happens before zeroization.

Alternatively, sensitive information used in a tactical scenario could be maintained entirely in an encrypted state. Warfighters would then pull, (i.e., decrypt) only the information needed at a particular time. The remainder of the disk or other storage device could remain encrypted until required by the warfighter, thereby limiting the amount of information that can be recovered by an adversary. This method involves file encryption, instead of the more extensive media encryption technique that would encrypt the entire storage media. Thus, a method for pulling subsets of information from an encrypted drive while maintaining encryption for the remaining data on the drive is also a tactical requirement. This solution would enable encryption of the storage media that is transparent to the user because of the limited amount of information stored in the clear at any point in time. Unlike zeroization, media encryption allows data recovery, enabling the soldiers to press the media encryption key first, so they can concentrate on defending themselves.

As stated previously, not all tactical information is perishable. Some data stored on tactical equipment may require more extensive protection because the sensitive nature of the data persists beyond today's operation. Examples of these types of data would be information on weapons systems, classified procedures, or other information that would remain classified long after the tactical operation is complete. Clearly, the user must first determine the perishability of the information before deciding on the strength of encryption required to protect the data.

## 9.3.2 Consolidated Requirements

- Tactical communications systems subject to theft or overrun by an adversary must have a real-time method of protecting sensitive information. Tactical information is often time sensitive or perishable. A decision must first be made about the perishability of the information. Then, the tactical user requires confidentiality services that can be rapidly applied to the information according to the sensitivity and perishability.
- A real-time means of protecting digital media must be available for the tactical user enabling the warfighter to quickly protect sensitive information in a time of crisis. Ideally, these services should operate transparent to the user.
- Near-term solutions using file encryption must have a method for pulling subsets of information from an encrypted drive while maintaining confidentiality for the remaining data on the drive.

## 9.3.3 Technology Assessment

Tactical success requires encryption hardware and software that can meet time-critical requirements and provide real-time encryption/decryption. Tactical systems must process encryption requests at speeds essentially equal to those of unencrypted requests. High-performance, real-time bulk encryption requires data rates that stretch the performance parameters of available hardware and software. Media encryptors specifically protect the confidentiality and integrity of data storage media. They are designed to encrypt the entire contents of the storage media (less certain system files in computers).

Generally, tactical equipment that is subject to recovery and exploitation by the enemy is better protected by media encryption versus file encryption techniques. Much tactical information is time sensitive and fast moving. Sorting out information for file type encryption is not feasible; thus protection of the entire storage media is more desirable. This process requires real-time media encryption to protect all the data in a timely manner. The wiring of the battlefield down to the individual soldier, and the enormous variety of communicated data, demands fast bulk media encryption and storage in a highly user-transparent manner.

Prime examples of the applications in the current technology are the developments in the FORTEZZA<sup>®</sup> family. Tactical applications for real-time encryption of mass storage devices including hard disks, floppy disks, tape drive, compact disc-read-only memory (CD ROM) and magneto-optical backup storage are coming on line. Promising COTS developments in dedicated Protocol Control Information (PCI) card encryption accelerators and faster algorithms coupled with tamper-proofing technology need to be integrated in a total protection package to reduce the threat of exploitation of recovered/captured equipment.

## 9.3.4 Framework Guidance

To meet this requirement in the near term, rapid media encryption can be accomplished on a file-by-file basis, rather than a total media encryption basis. However, this method does not provide the desired degree of assurance that the OS has not made duplicate copies of sensitive information in temporary files. This Framework recommends further developments of trusted OSs, as well as faster media encryption technologies that will operate transparent to the user.

## 9.4 Key Management in a Tactical Environment

Overall key management for a tactical communication network involves generation, distribution, and storage of keying materials. Clearly, this process requires an extensive key management infrastructure (KMI) to handle the number of users in a tactical environment. Fortunately, the U.S. military has spent many years improving the current KMI used to distribute symmetric keys to troops around the world. Entire documents have been written on the structure of the military's KMI. This document does not describe the entire key management process; instead, it discusses some of the current issues related to key management in a tactical environment. These issues include black key transfer, remote rekey, transfer, zeroize functions, and key loading functions.

Remote rekey has become a major IA issue in recent years for several reasons. The capability of a user to rekey COMSEC equipment from a remote location eliminates the need to either bring equipment to a central location, or send key updates to field locations. Any dangers of key compromise along the shipping process are eliminated, along with drastically reducing the time required for key updates. More importantly in a tactical situation, if a node in a network should be compromised, a good network management and control system can lock out compromised nodes and remotely rekey all other nodes in a network. Thus, an adversary who obtains keys and communications equipment cannot listen to sensitive communications or attempt spoofing attacks against friendly forces by pretending to be a valid user on the net.

### 9.4.1 Mission Need

One of the primary concerns for the warfighter is the elimination of red key. The current Electronic Key Management System (EKMS) delivers black key from the Central Facility to the Local Management Device/Key Processor (LMD/KP). For the tactical Army, this brings keys down to the division level in a benign, secure manner. However, transfer of keys from division down to brigade, battalion, and below is performed by a soldier carrying a key fill device, such as the Data Transfer Device (DTD), full of red keys. This soldier is a target waiting to be exploited. Thus, the tactical warfighter requires a KMI that can receive black keys all the way down to the end COMSEC unit. That is, there should be no point in the transfer of keys where they are stored red. This will minimize the risk of insider attack and ease compromise recovery.

## UNCLASSIFIED

Information Assurance for the Tactical Environment  
IATF Release 3.1—September 2002

Remote rekey and network management can be accomplished with over-the-air rekey (OTAR) or across a landline, as with a STU-III or STE. Over-the-air zeroize (OTAZ) and over-the-air transfer (OTAT) of keys are closely related to OTAR. These processes involve the rekey, zeroize, and transfer of keys across a communications link from a centralized key management center to deployed COMSEC equipment. One IA challenge with these processes is how to confirm the identity of the network control station and the end-user equipment. Without proper identification and authentication (I&A) services, a sophisticated adversary could conceivably impersonate the network control station, send out a key update, and take control of part of the tactical network. Therefore, the first requirement for OTAR systems is to implement high-assurance key management capability, using remote rekey mechanisms in tactical networks to ensure access control, integrity, and confidentiality for the rekey message.

The second requirement for OTAR systems is an automated process for conducting OTAR that can run on any tactical automation system, such as the Maneuver Control System (MCS). An operator at the key management center would program the software to automatically send out new keys at a designated time. Any system that does not acknowledge receipt is identified quickly by the OTAR system, and the status of that particular unit or individual would then be verified. These types of systems exist for the Data Encryption Standard (DES) and other Type III federal systems but not for Type I tactical systems.

Third, a common key fill device is required to operate with multiple types of cryptographic keys and multiple end systems. If the tactical user requires three or four different key loading mechanisms in the field, units must bring extra COMSEC equipment to the field. With a single-key fill device, this equipment burden could be reduced drastically.

Remote keying mechanisms are essential to eliminating the need to bring large numbers of COMSEC items to the field. For example, implementing OTAR and OTAT mechanisms, a unit would only need the initial key fill for COMSEC equipment deploying to the field. All other updates would be accomplished remotely. If tactical forces operating in hostile territory rely on remote keying, the chance of an enemy gaining access to COMSEC keys would decline significantly. However, remote keying places a high degree of trust in the key management and network management functions. If tactical units rely on an automated system to send out key updates, significant IA must exist within the automated system. Tactical forces must have total confidence in the rekey process. Forward units must know that the enemy cannot spoof the network management station by sending out false COMSEC updates to friendly equipment. If there is any doubt about the validity of keying information, units may choose to operate “in the clear,” without encryption, instead of possibly accepting a rekey from hostile forces.

Additionally, if any tactical COMSEC devices or keys are captured, all other nodes on communication nets using the compromised keys must be notified immediately. Many of these processes are in place today for single-key types in legacy cryptographic systems. However, the process is not as clear for public key infrastructure (PKI) and reprogrammable cryptographic devices handling keys for multiple networks. Improvements in I&A of network control stations will provide a much higher degree of assurance that the enemy has not spoofed a network control station. A final requirement is the development of a KMI to deal with EKMS, PKI, and reprogrammable cryptography. Additionally, to fully realize the potential of programmable

cryptography, current COMSEC algorithms should be integrated into programmable COMSEC chips.

## 9.4.2 Consolidated Requirements

- Tactical users require the development of a KMI to deal with EKMS, PKI, and reprogrammable cryptography. High-assurance remote key management capabilities must be implemented in tactical networks, including methods for conducting OTAR, OTAT, and OTAZ. Additionally, processes must be established to disseminate compromised key information for PKI and reprogrammable cryptographic devices handling keys for multiple networks.
- Tactical users require a process to transfer black key all the way down to the end COMSEC unit on the battlefield, dramatically reducing the vulnerability of key compromise.
- High-assurance I&A services must exist for both network control stations and end users for OTAR, OTAT, and OTAZ.
- Tactical users must have an automated process for conducting OTAR that can run on any tactical automation system.
- Tactical users must have a common key fill device to operate with multiple types of cryptographic keys and multiple end systems.

## 9.4.3 Technology Assessment

This section focuses on technologies associated with key loading, remote rekey, OTAR, OTAZ, and OTAT. A section on PKI has been added to address the movement to public keying in future DoD systems.

OTAR is not a new topic for tactical communications systems. The Army's mainstay radio system, Single Channel Ground and Airborne Radio System (SINCGARS), has a remote rekey capability. Other systems throughout DoD also have this capability. The issues discussed in this section are specific to certain aspects of remote keying, including Type 1 automated tactical OTAR, Type 1 OTAZ, the development of a single-key fill device, and development of a common compromise policy and recovery method for programmable cryptography devices.

OTAR is an effective way to distribute key updates to deployed forces in a tactical scenario. It reduces the amount of keying material that must be transported to the field, which increases the risk of key compromise. Additional improvements to the OTAR process should focus on developing an automated process for conducting OTAR that can run on any tactical automation system (such as the MCS). An operator at the key management center would program the software to automatically send out new keys at a designated time. Any system that does not acknowledge receipt is quickly identified by the OTAR system, and the status of that unit or

individual would then be verified. These types of systems exist for DES and other Type III federal systems, but not for Type I tactical systems.

In contrast to OTAR, very few OTAZ schemes are approved for military radio systems. A common scheme should be developed for use in all future DoD tactical radio systems. Similarly, there is no single-key fill device available to support the variety of COMSEC systems fielded. With different key fill devices available for Type I, Type III, public key, and commercial key systems, a tactical unit often carries a multitude of fill devices to the field. A common fill device would lighten the load for the warfighter, and reduce the requirement to protect and store the additional devices. Some devices currently used for downloading keys to COMSEC devices are the DTD, KYK-13, KYX-15, or KOI-18. The DTD is probably the most interoperable key loading device currently used, compatible with such COMSEC equipment as SINCGARS radios, VINSON, KG-84, and others that are keyed by Common Fill Devices (CFD). The next version of the DTD, the DTD 2000, is under development.

Another requirement that must be met by a tactical key management system is a common compromise and recovery policy. If programmable cryptographic devices are used in tactical radios of the future, each unit may have radios keyed for multiple networks. The specific networks may vary from unit to unit or from one contingency to another. As an example, if a radio is compromised with keys for SINCGARS, HaveQuick, and Enhanced Position/Location Reporting System (EPLRS) nets, a chain of notification, including the designated key compromise authority for each type of key, needs to be identified. A set time for key changes and a new key distribution schedule need to be identified as well.

## Public Key Infrastructure

Success in accomplishing the mission in the tactical environment depends to a large degree on the establishment of a secure means of moving information resources—data, voice, and imagery—to support the effort. Implementing a PKI will certainly not solve all tactical IA problems. However, a robust PKI could become a critical component of a fieldable IA solution for battlefield and other tactical operations.

PKI allows tactical users to interact with other users and applications, to obtain and verify identities and keys, and to provide other authentication services. There are three primary levels of assurance: high, medium, and basic. In the DoD, PKI certificates will be issued for medium and high assurance only. DoD has no plans to support a separate basic level infrastructure. This is not to imply that PKI services at the basic level of assurance will not be of importance to DoD, only that these services will be provided by the medium assurance infrastructure. High assurance is provided by Class 4 certificates such as FORTEZZA<sup>®</sup> cards. High assurance devices are generally hardware-based tokens providing protection for Unclassified but Controlled mission-critical information over unencrypted networks (Type 2 information). Medium assurance refers to software-based end-user tokens (Class 3 certificates) requiring in-person or trusted agent registration that will eventually migrate to a common smart card such as the DoD identification card. Medium assurance certificates can protect less sensitive information such as support and administrative information. Basic assurance refers to lower

## UNCLASSIFIED

Information Assurance for the Tactical Environment  
IATF Release 3.1—September 2002

assurance, software-based solutions providing minimal protection because of the lack of registration controls.

A critical issue for tactical communications is interoperability over a wide range of vendors' products and standards. This is compounded by the likely requirement to interoperate with a large number of PKIs from allied military forces and other elements of the U.S. and allied governments. These other PKIs may be based on different products, certificate policies, and algorithms. Technology in this area is still evolving. Key tactical issues such as compromise recovery, key recovery, and rapid personnel transfers must be addressed. Public key cryptography is one of the most promising emerging technologies, but the Framework required to support a viable PKI, needs to be carefully thought out and established.

### 9.4.4 Framework Guidance

Key management in a tactical environment has been handled by the Services for many years for symmetric key types. However, as the DoD moves closer to adopting a total PKI solution, tactical key management also will require modifications. This Framework strongly recommends that any new system under development be able to receive black key all the way down to the end COMSEC unit. In other words, there should be no point in the transfer of key where it is stored red. This will minimize the risk of insider attack, decrease the risk to the warfighter carrying red key, and ease compromise recovery. Current systems that provide an OTAR capability (e.g., SINGARS) should continue to take advantage of their remote rekey functionality. As interoperability between networks increases, the Services must work to develop a common compromise and key recovery policy for use with tactical systems loaded with multiple COMSEC keys for different networks. This technology gap will be particularly important as tactical communications equipment begins to implement programmable Information Systems Security (INFOSEC) devices. Furthermore, a single key fill device for all tactical COMSEC equipment does not exist. Industry should focus on this area in the near future. Finally, this Framework encourages the continued development of programmable cryptographic devices, and the implementation of current COMSEC algorithms on these devices. Future systems such as JTRS will play a key part in not only the use of programmable cryptographic devices, but also the refinement of current key management policies and procedures in the tactical arena.

## 9.5 Network Mobility/Dynamic Networks

U.S. tactical forces conduct a majority of their operations in locations outside the CONUS. Therefore, a need exists for these forces to maintain seamless network connectivity regardless of location. In the civilian world, a business traveler can remotely access his or her company's network from anywhere in the world through a dialup remote access connection or by simply acquiring an Internet connection at the mobile location and accessing files and e-mail through a network connection. In either case, tracing phone numbers or IP addresses can trace the traveling businessman to a specific location. Such location tracking is not desirable for a tactical user because specific locations of tactical units are often sensitive, if not classified.

## 9.5.1 Mission Need

Consider the case of establishing a deployed LAN with an Internet server. A new host IP address must be assigned at each location, forcing frequent updates of the Domain Name Server (DNS). One requirement for mobile tactical users is the capability to seamlessly connect to a local subnetwork anywhere in the deployed tactical network. Tactical operations often combine equipment from different units, forming several different subnets. Users need continuous access to the network as they move between subnets, regardless of which unit “owns” the subnet. The tactical user does not have time to reconfigure local IP address information every time the subnet changes. Furthermore, IA technologies must exist to protect the packets against active and passive attacks by unauthorized individuals from both the home and foreign subnets visited by the tactical user. Although making it easier for authorized users to travel between subnets, the deployed tactical network must still employ IA mechanisms that authenticate mobile users to prevent the adversary from gaining access somewhere in the network.

A different, but related, mobility requirement for tactical forces is the need for rapid setup and teardown of communications networks. Tactical network applications differ from fixed plant applications in that tactical networks are mobile. Tactical units rarely stay in the same location for the duration of an operation. Therefore, networks that require vast amounts of cabling are often impractical for use in a tactical operation. To the extent possible, bulky cabling should be replaced by wireless solutions in future highly mobile systems. Of course, wireless systems present additional challenges such as jamming and geolocating that also must be addressed. The point is that security services should not increase equipment setup time for the warfighter. Secure wireless network solutions for tactical applications are a key area for industry development. IATF Section 5.2, Wireless Communications, discusses wireless systems.

Tactical mobility can also be achieved by using global broadcast communications systems and UAVs used as communications nodes. Although these topics apply to tactical network mobility, they are covered more specifically in Section 9.7, Secure Net Broadcast/Multicast.

A Tactical Operations Center (TOC) is today’s central communications hub for most Army tactical information systems. Setting up a TOC and running all the required cabling can take from 24 to 48 hours. This is too long. Therefore, rapid setup and teardown can become a major issue. An airborne unit may have more of a challenge with TOC mobility than a less mobile Army unit because an airborne unit is considered a “shoot and move” unit, requiring a more mobile TOC. In this situation, full communications capability can lag behind the unit because of the time required to setup a TOC. Replacing cabling with wireless connections would drastically decrease set up time. Additionally, wireless solutions allow the creation of a *mobile* TOC, installed in a set of three or four vehicles, with communications staying “up and running” while the TOC is on the move. The U.S. Army’s First Digitized Division is attempting to implement a mobile TOC in several vehicles with wireless bridges and TACLANE encryptors. The TACLANE encryptor is discussed later in this section.

Regarding mobile networking, the security implications depend on the type of tactical application in question. Without dynamic networking solutions in place, seamless message

## UNCLASSIFIED

Information Assurance for the Tactical Environment  
IATF Release 3.1—September 2002

addressing is more difficult. Individuals sending messages to tactical forces must know the network address of the recipient before sending a message. Also, an adversary may more easily locate U.S. forces at deployed locations by watching message headers flowing across a network. However, not all tactical units are particularly concerned about the enemy knowing their location. Thus, this issue will vary in importance depending on the particular tactical information system application.

Mobile wireless networks have an increased possibility of eavesdropping, spoofing, and denial of service attacks. The mobile networking concepts under development must account for information security hazards such as these in their development phase. For example, in an IP network, routers continuously broadcast routing tables to other nodes in the network to help other routers choose the best route to send IP packets. However, if this broadcast is done in the clear on a wireless net, an adversary could quickly glean an approximate picture of the layout of the tactical network. A second challenge in applying these technologies in the tactical arena involves incorporating routing and security functionality in smaller form factors such as handheld radios. Size, weight, and power requirements for computer equipment will continue to decrease as technology improves, which may help alleviate this issue. Future tactical equipment will require secure protection for over-the-air exposure of user information, addressing, system control information, and portable processing. Where routing functionality is provided in addition to the traditional radio applications, routing tables must be transmitted on a secure channel that all nodes in the network can access.

Finally, new mobile ad hoc networking technologies must remain backward compatible with certain legacy communications equipment. Even as new technologies become available, tactical units will retain much of their legacy communications equipment because of large upgrade costs and experience with current systems. Thus, legacy radio addressing will remain a key issue to consider when developing new mobile networking technologies.

### 9.5.2 Consolidated Requirements

- Tactical users must have the capability to maintain seamless network connectivity regardless of location or subnet. Network routing and domain name servers must have the ability to forward data to tactical users moving between networks. Users require continuous access to the subnets as they move through the field.
- IA protections for tactical networks must be flexible enough to operate on different types of equipment from various units worldwide.
- IA solutions must prevent access to any subnet by unauthorized users.
- Many tactical users require protection against geolocation by an adversary. Therefore, dynamic networking solutions must provide confidentiality for specific location information where necessary.

- Tactical communications equipment must be capable of rapid setup and teardown, allowing greater mobility for the tactical unit. Security solutions should be applied in smaller form factors (e.g., handheld and man-portable).
- Mobile networking concepts developed for the tactical environment must address passive and active attacks from a sophisticated adversary.
- Tactical wireless solutions should implement Low Probability of Intercept (LPI), Low Probability of Detection (LPD), and Antijam (AJ) technologies to provide transmission security (TRANSEC) as required for the particular tactical mission.
- Advanced networking technologies must remain backward compatible with major legacy communications systems and equipment.

### 9.5.3 Technology Assessment

Significant advances in mobile IP technologies have made several of these tactical mobility requirements a reality. As discussed in IATF Section 4.4, Important Security Technologies, Internet Protocol Security (IPSec) used in mobile IP enables a mobile node to change its attachment point on the Internet while maintaining its IP address(es) and protecting its communications when visiting foreign subnets. Traveling between subnets resembles a cellular user roaming from one cell to another. However, future advances in mobile wireless communications will likely involve the use of the IP suite. Using IP in a cellular-like roaming situation creates several IA issues that must be solved.

The message originator wants assurance that a message will reach the correct destination, regardless of the physical location of the recipient, without any chance of interception or spoofing by an adversary. This also must be true, even when the originator does not know the location of the recipient. Likewise, a recipient must ensure that received messages from the “commander” are indeed from the commander, regardless of where in the network the commander is located. In an attempt to solve these assured delivery and nonrepudiation problems, a concept of mobile ad hoc networking (MANET) has been developed to support robust and efficient operation in mobile wireless networks by incorporating routing functionality into mobile nodes. Such networks are envisioned to have dynamic, random, multihop technologies that are likely composed of relatively bandwidth-constrained wireless links. This vision differs from Mobile IP technologies in that the goal of mobile ad hoc networking is to extend mobility into the realm of autonomous, mobile, and wireless domains, where a set of nodes, which may be combined routers and hosts, form the network routing infrastructure in an ad hoc manner.

#### Mobile IP and MANET

MANET is an autonomous system of mobile routers and associated hosts connected by wireless links. The routers are free to move randomly and organize themselves arbitrarily, thus allowing the network’s wireless topology to change rapidly and unpredictably. Such a network may operate in a stand-alone manner or may be connected to the larger Internet. [1] These nodes

## UNCLASSIFIED

Information Assurance for the Tactical Environment  
IATF Release 3.1—September 2002

principally consist of a router, which may be physically attached to multiple IP hosts or IP addressable devices. This router may have potentially multiple wireless interfaces, each using various wireless technologies. [1]

Mobile nodes are mobile platforms that make up a MANET. These nodes may be located on airplanes, ships, trucks, and cars. The MANET system may operate in isolation or may have gateways to interface with a fixed network. The MANET system consists of dynamic topology. With this topology, nodes are free to move arbitrarily; thus, the network topology, which is typically multihop, may change randomly and rapidly at unpredictable times and may consist of bidirectional and unidirectional links. The decentralized nature of network control in MANETs provides additional robustness against the single points of failure of more centralized approaches. [2] MANETs also have limited physical security. Mobile wireless networks generally are more vulnerable to physical security threats than cable networks. There is an increased possibility of eavesdropping, spoofing, and denial of service attacks with wireless networks.

This protocol permits mobile internetworking to be performed on the network layer; however, it also introduces new vulnerabilities to the global Internet. First, the possibility exists for an adversary to spoof the identity of a mobile node and redirect the packets destined for the mobile node to other network locations. Second, potentially hostile nodes could launch passive/active attacks against one another when they use common network resources and services offered by a mobility supporting subnet. The first vulnerability can be surmounted by the strong authentication mechanisms built into both basic Mobile IP and route optimized Mobile IP. [2] By using PKI, a scalable countermeasure against the spoofing attack can readily be deployed. An effort is under way to surmount the second vulnerability.

Mobile IP and mobile nodes have several requirements to allow for maximization of security. First, when a mobile node is on its home network and a Correspondent Host (CH) sends packets to the mobile node, the mobile node must obtain these packets and answer them as a normal host. However, if the mobile node is away from its home network, it needs an agent to work on its behalf. [3] The second requirement is that of the expectation of the mobile nodes to retain their network services and protect their communications when they visit foreign subnets and the expectation of the foreign subnets to protect their network resources and local traffic while they are visited by the mobile nodes. A mobile node roaming over the Internet should have safe and persistent IP connectivity that is permitted by the policies of its home and visiting subnets. Persistency of IP connectivity means that the connections should be handed off quickly and correctly so that the mobile node can maintain its Transmission Control Protocol (TCP) sessions when it changes its network attachment point. [4]

Additional information about Mobile IP is available at Web site:

[http://www.hpl.hp.com/personal/Jean\\_Tourrilhes/MobileIP/](http://www.hpl.hp.com/personal/Jean_Tourrilhes/MobileIP/). [3] For additional information about MANET, visit Web site <http://www.ietf.org/html.charters/manet-charter.html>. [1]

## TACLANE/FASTLANE/TACLANE Internet Security Manager

In an effort to overcome some of the drawbacks and interoperability issues with current bulk encryption technologies, two Type 1 IP and Asynchronous Transfer Mode (ATM) encryptors have been developed for the National Security Agency: TACLANE (KG-175) and FASTLANE (KG-75). These encryptors provide access control, authentication, confidentiality, and data integrity for individuals or groups of users. TACLANE encryptors are more likely to be used in a tactical scenario because of size and mobility issues. The Army's First Digitized Division uses TACLANE encryptors with a wireless bridge to set up a wireless tactical operations center among a suite of vehicles.

The TACLANE encryptor will secure communications in a dynamic TPN, in the Defense Information Systems Network, or over the Internet, facilitating integration of these and other mobile and fixed networks. This encryptor operates at 45 Mbps for ATM networks and 4 Mbps for IP networks. A new, smaller version of the encryptor, "TACLANE Lite," is a PC card size device that is compatible with TACLANE. The PC card version supports data rates from 1 to 45 Mbps. The reduced size, weight, and power will allow greater operational interoperability.

These encryptors support different levels of secure transmission by employing crypto-ignition keys, much like a STU-III or a FORTEZZA card in the STE. When the CIK is removed, the encryptors are Unclassified/CCI. As mentioned in Section 9.2, Wiping Classified Data From Tactical Equipment, changing the assigned classification level of a CIK is possible, but it requires a significant amount of time (potentially several days). Ideally, future systems will be able to operate at multiple security levels without undergoing a lengthy rekey process. The real strength of these encryptors comes from the integration of the TACLANE Internet Security Manager (TISM) in the tactical network. The TISM allows remote management of encryptors and their protected devices from a central location.

The TISM provides remote rekey of the FIREFLY keying material in the TACLANE and FASTLANE encryptors, reducing the chance of compromise by eliminating manual distribution of keys. Also, FIREFLY and traditional keys can be assigned to FASTLANE and TACLANE ATM virtual circuits with the ability to activate and deactivate them. Furthermore, audit data from encryptors throughout the network can be collected and reviewed in a central location, looking for errors or evidence of electronic attack on the network. A TISM operator can specify alternate TISM managers as a backup. If a TISM site is compromised or overrun, network management can be conducted from an alternate location. Future enhancements to the TISM include remote zeroization capability and electronic distribution of access control lists.

### 9.5.4 Framework Guidance

Until secure, wireless network solutions are implemented, tactical units will continue to use copper and fiber connections to connect local network nodes. Minimal security challenges arise using copper and fiber instead of wireless. The major drawbacks are longer equipment setup and teardown times and larger lift requirements as a result of the weight of the cabling. On the other hand, there can be a greater risk of jamming and geolocation when using wireless solutions.

Thus, tactical wireless solutions should implement LPI, LPD, and AJ TRANSEC as required for the particular tactical mission. System integrators for tactical organizations should also note continuing developments in the mobile networking arena. Many lessons can be learned from the Army's First Digital Division because they implement mobile wireless networking technologies and TACLANE encryption devices. Dynamic addressing schemes will also play a key role in improved communications for mobile users.

In addition, Personal Communications Systems (PCS) on the battlefield are currently in the form of small lightweight cells. This allows the tactical user limited mobility in the Division and rear areas. PCS radio access points and cell sites need to be small and rugged enough to be mounted on vehicles that travel with the tactical users. These cells would have to operate with little or no operator involvement, and the mobile networks would have to be self-configuring as the mobile cells move with respect to their users.

## **9.6 Access to Individual Classified Accounts by Multiple Users**

Information systems often make use of shared directories or databases that can be accessed by a group of users for a specific purpose. Users expect to have individual e-mail accounts for sending and receiving messages, files, and other critical information. However, military and other tactical units tend to operate more as a group focused on a particular mission. When communicating with a unit, messages are sent to a particular position, or function within that unit (e.g., Commander or First Sergeant) as opposed to being sent to some specific individual by name (role-based access control versus individual access control). Unfortunately, this means a higher risk of messages or data ending up in inappropriate hands. This is a key concern if an insider threat exists within a unit. With recent advances in access control technologies, significant limitations can be placed on who (by name or by role) may access a particular account, file, or database. Thus, the danger of message traffic ending up in inappropriate hands is eliminated. These access control technologies work well in the commercial world, but it is unclear how well they transfer to tactical operational environments.

Communications systems of the past typically used role-based access control mechanisms, partially because of a lack of sophisticated individual access control technologies, and because of the need for accessibility by several operators on different shifts. Today, the standard password controls can be used in concert with other technologies such as biometrics (fingerprint, retinal, or iris scanners), PKI mechanisms (hardware and software), or other cryptographic tokens. Some of these methods present unique IA issues regarding access to information by a limited number of individuals. These potential solutions are discussed in more detail later in this section. The network must have the ability to uniquely recognize each individual in a tactical scenario and allow that individual access to information in accordance with his or her role-based need to know.

## 9.6.1 Mission Need

In a tactical scenario in which a commander or other key individual could be replaced, captured, or killed, the chain of command is defined so the next person in the chain will assume command seamlessly. If Commander A is removed from the picture, Deputy Commander B must be able to assume command and have access to all messages and files that Commander A had. If the Commander is the only person with the “key” and is captured, the Deputy Commander cannot effectively make command decisions because of a lack of information. Similar single points of failure may exist with system administrators or other critical positions.

As illustrated in the above scenario, new users/commanders must be able to access the same message and database capabilities as former users/commanders. Without the proper multiuser access control technologies in place, one of two outcomes will result. Either the unit will choose not to use the access control mechanisms for the communications equipment, or the unit will risk not having access to critical information if key authorized individuals are unavailable. Therefore, tactical information systems require a fieldable network access control mechanism with an ability to uniquely recognize each individual in a tactical scenario and allow that individual access to information and system use capabilities in accordance with that required and authorized for their role.

In the past, tactical units have typically chosen to use either widely disseminated passwords that are rarely changed, or no access control mechanisms at all. Physical security controls governed which individuals had access to specific information or message services. Unfortunately, enemy capture of equipment has occurred, and enemy forces often became adept at using captured equipment to impersonate U.S. forces on U.S. radio channels. As a result, complicated and burdensome authentication schemes were devised to defeat these impersonation attempts. It is unknown how successful these authentication schemes were. Current tactical communications systems increasingly relay data without operator intervention and must rely on more sophisticated access control systems that provide a high degree of assurance regarding authentication of distant ends. Tactical users must make split-second decisions that could have grave consequences. If the user suspects that distant end access control has been breached, messages received over the network will not be trusted. Furthermore, any new access control mechanism to be fielded in a tactical environment should be simple and reliable enough to assure the user that information is secure. As with any new technology, new tactical communications networks must earn the user’s trust before reaching their full potential.

## 9.6.2 Consolidated Requirements

- Access control services on tactical equipment must be flexible enough to uniquely recognize each individual and allow that individual access to information based on clearance level and current mission needs.
- Any access control mechanism must be simple and reliable enough to operate in a tactical environment and to assure the user that authentication information is secure.

## 9.6.3 Technology Assessment

IA solutions for this issue continue to develop rapidly. As stated in Section 9.6.1, Mission Needs, any solution must be able to uniquely identify users and grant them access to information in accordance with their individual clearance level. Possible solutions include implementing smart card technology on DoD identification cards, maintaining and using biometric information on all individuals involved in tactical situations, or assigning public key certificates to all DoD personnel reflecting authorized security levels. PKI solutions are described in Section 9.4.3, Technology Assessment. Other technologies are described below.

### DoD-Wide Certificates

DoD plans to issue public key certificates to all military personnel for identification and encryption purposes. By direction of the Deputy Secretary of Defense, all DoD users will be issued, as a minimum, Class 3 (medium assurance) certificates by October 2001. Beginning in January 2002, the Class 3 certificates will be replaced by Class 4, high assurance certificates for all DoD users. [5] DoD PKI medium assurance certificates located on smart cards or floppy disks are starting to be used by DoD personnel interfacing with the Defense Finance and Accounting Service (DFAS). These certificates could transfer well to a tactical network application to validate the identity of system users and the authenticity of messages received from those users. The primary reason certificates exist is to associate individuals with their public key. [6]

### Biometrics

Biometrics is the statistical analysis of biological observations and phenomena. Biometrics identity verification systems use biometrics as a method for recognizing a person by measuring one or more specific physiological or behavioral characteristics, with the goal of distinguishing that person from all others. Biometric devices must be based on a characteristic that differs in a measurable way for each user. Characteristics that meet this criterion are iris scans, hand geometry, deoxyribonucleic acid (DNA), and fingerprints.

The application of biometric technology in fast moving tactical situations offers some clear advantages. Tokens, smart cards, and physical keys can be lost, stolen, or duplicated, and passwords can be easily forgotten or observed. Only biometrics bases I&A on an intrinsic part of a human being—something that is always available and totally unique.

Applications are coming into use in the commercial and the civilian sectors of the federal and state government. Current military applications, to date, are sparse and appear to center more on use in fixed facilities as opposed to purely tactical applications. However, as the technology progresses, several tactical applications are likely to arise for biometrics. Much of this is anticipated because biometric devices are expected to become widespread in the commercial and government sectors in the next few years. Although biometric applications have been available for many years, recent reductions in the cost of biometrics devices and the introduction of new applications (i.e., controlling network login, Web server access, and media encryptor access) are

driving the deployment of biometric devices. Current shortfalls in the technology related to a tactical environment are as follows:

- **Lack of Standardization.** The government and commercial industry are working together to define a standard for biometric products. The Biometrics Application Program Interface (BAPI) will allow products from multiple vendors to interoperate, preventing one-vendor solutions. Products adhering to the BAPI standard are expected in the near future.
- **Environmental Conditions.** Environmental conditions in a tactical environment may reduce the effectiveness of some biometrics devices. For example, heavy rain may affect facial scanners, dirt or injuries may affect fingerprint scanners, or loud noises may affect vocal recognition devices. These conditions may affect the accuracy of the biometric devices. The use of biometric devices by tactical users wearing protective garments such as gas masks must also be addressed.
- **Computing Power.** Advances in computing power and in biometrics recognition techniques have reduced the computing power required by biometric devices making biometrics more attractive and affordable for strategic environments. However, the low power, low-computing power tactical user may not be able to perform biometric verifications in a timely manner.

Despite these current limitations, biometrics offer some interesting future possibilities for tactical applications. As biometric devices become transportable, the possible applications for a tactical environment become feasible. For example, military units frequently shared equipment, databases, and directories. Access to individual files and databases must be restricted to authorized users only. Biometrics could provide the unique discriminator necessary to restrict access to the authorized user. Users could carry their biometric signature on a smart card. When they require access to a system, they would insert their smart card, scan their biometric trait, and gain access to the system. Each user carrying his or her biometric on a smart card could provide a strong authentication mechanism that is transportable across multiple units.

## 9.6.4 Framework Guidance

Until DoD realizes the full implementation of DoD PKI, tactical units should continue to use the role-based access control mechanisms in use today. In situations in which one password is shared among multiple users, system administrators should assign unique usernames and passwords to each individual to decrease the chance of password compromise, even though each individual has identical access privileges. Advances in biometric authentication products may or may not prove useful in the tactical arena. ISSEs and system integrators should pay close attention to new developments in this area to determine what applicability they might have to tactical communications systems.

## 9.7 Secure Net Broadcast and Multicast

DoD, military, and civil agencies conduct numerous operations that involve the use of tactical broadcast equipment. These operations can range from U.S. military troops actively involved in war to law enforcement officials conducting a drug raid or seizure. The term “secure net broadcast” refers to a networked communications system where all transmissions from any node in the network can be received by every other node. For voice communications, this network resembles the Citizens Band (CB) radios used in the trucking industry. However, in a tactical environment, broadcast transmissions must maintain confidentiality and integrity during transmission to prevent interception by an adversary. Similarly, multicast transmissions are directed at a subset of nodes in a network. From the early entry phases and throughout the lifetime of tactical missions, voice and data information must be broadcast and multicast to multiple nodes securely and accurately. The tactical equipment used in these exercises must allow users to move rapidly with flexible and survivable voice and data communications.

### 9.7.1 Mission Need

Traditional land mobile radio (LMR) systems may not have the range to handle broadcast communications over a large area; other broadcast and multicast solutions may be required. Several technologies, such as CONDOR, UAVs, Global Broadcast Service (GBS), and PCS, exist to help reduce these vulnerabilities. These technologies provide point-to-multipoint security solutions for wireless communication systems. They also secure data broadcast and multicast by providing a high-bandwidth communications networking infrastructure. In addition, several of these technologies use direct broadcast satellite technology to prevent data interception or jamming.

As mentioned previously, voice and data broadcast and multicast in a tactical environment are subject to many vulnerabilities. Whether it is a military troop in a hostile environment engaged in war or a civil agency performing a drug seizure, operational data must be kept secure and accurate while in transmission from one point to another. During data broadcast and multicast, the data could be intercepted, altered, or jammed if not adequately protected. Any of these vulnerabilities could result in fatalities. For example, in a tactical environment, troops and law enforcement officials attempt to remain undetected while executing the mission or exercise to prevent geolocation, insertion of false messages, or communications jamming, thus giving an adversary the advantage. Any of these threats could lead to disaster for any mission or exercise.

### 9.7.2 Consolidated Requirements

Tactical communications equipment must allow operators to roam over a wide area and still be able to receive and send secure broadcast and multicast data over the local infrastructure. Secure network broadcast and multicast systems include the following security services requirements:

- Tactical users on the move must be able to send and receive voice and data information in a secure and undetectable manner. The minimum acceptable data rate for voice broadcast is 2.4 kilobits per second (kbps).
- During the broadcast and multicast of voice and data information, this information must be protected from detection and identification, transmission jamming, geolocating, RF signal attacks, infrared (IR) signal attacks, and message insertion and modification.
- Tactical communication equipment must be capable of performing rapid, secure broadcast and multicast of high-volume military information such as maps, intelligence data, weather reports, and air tasking orders.
- Tactical communications equipment must have improved filtering to combat interference and jamming that will require advances in Digital Signal Processing (DSP).

### 9.7.3 Technology Assessment

Various security technologies have been developed to improve secure voice and data broadcast and multicast. These security technologies help to reduce the vulnerabilities identified in Section 9.7, Secure Network Broadcast and Multicast.

#### CONDOR

The CONDOR Program provides security in wireless telecommunications systems to meet the communication security requirements of DoD, military, and civil agencies. CONDOR provides point-to-multipoint security solutions for secure network broadcast and multicast service using the FNBDT signaling plan to connect various communications systems, including IS-95 (Code Division Multiple Access [CDMA]), Advanced Mobile Phone Service (AMPS) CypherTac 2000 and the mobile satellite systems of Iridium, Globalstar, and ICO. This signaling plan is also interoperable with the tactical and office STEs. CONDOR phones could prove useful as a broadcast voice solution for tactical commanders on the battlefield. Commanders could have a mobile conferencing capability from any location within the tactical cellular network. For additional information about CONDOR and its technologies, visit the following site: <http://condor.securephone.net>. [7]

#### Unmanned Aerial Vehicle

UAVs used as cell stations will help provide secure network broadcast and multicast communications for the tactical user. UAVs can provide a high-bandwidth, robust, and multimedia theater-level communications networking infrastructure that will protect net data broadcast/multicast from the vulnerabilities of jamming and interception. Currently, UAVs are used primarily as photoreconnaissance platforms. However, to fully use the UAV on the battlefield, the UAV should be used as a cell station, or Airborne Communications Node (ACN). A tactical cellular network could be rapidly established by simply launching the UAV. From an altitude of 20,000 or 30,000 feet, an ACN produces a much larger cell area than a standard cellular tower. The UAV used as an ACN in the tactical Internet can provide warfighters with secure multimedia high-bandwidth Internet-type communications support in hostile tactical

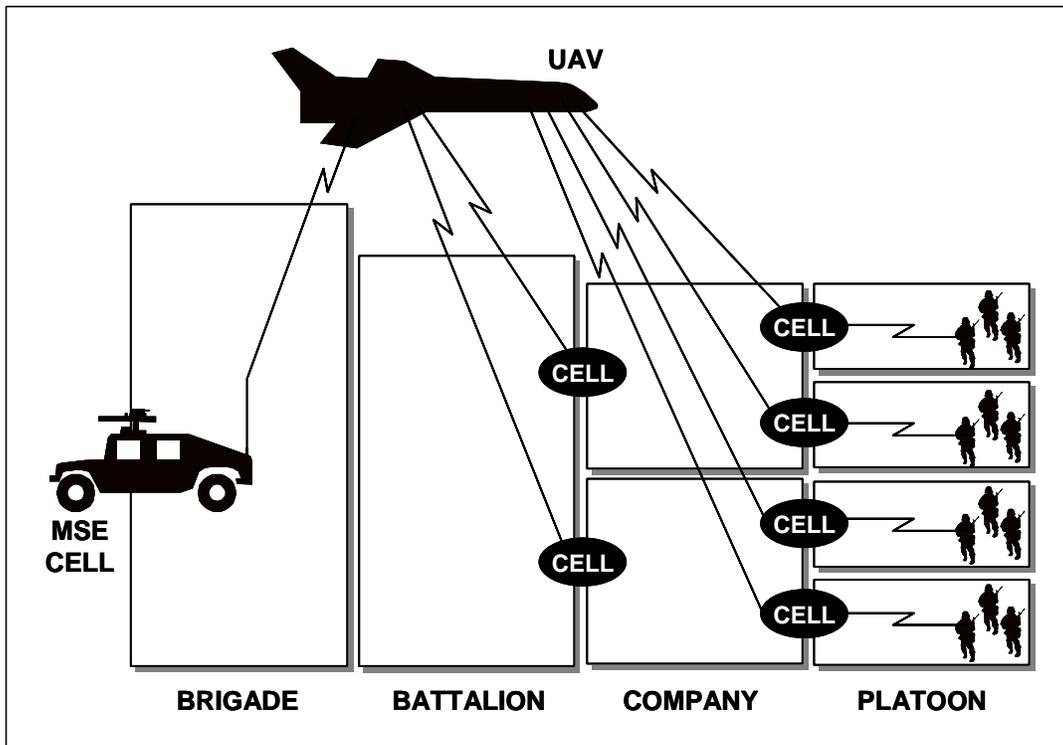
environments where communications must be broadcast and or multicast to various destinations securely and accurately. For additional information on how UAVs can provide secure net data broadcast and multicast, visit <http://www.darpa.mil>. [8]

## Global Broadcast Systems

GBS, developed by DoD, will increase the amount of national and theater-level information broadcast and multicast to deployed forces involved with operations in tactical environments. As the amount of broadcast and multicast data increases, GBS also provides increased security by using direct broadcast satellite technology. GBS enables commanders at the main operating base to transfer vast quantities of information to forward units. This technology protects the data from vulnerabilities such as interception, jamming, and modification.

## Personal Communications Systems

PCS technology products have been developed to send and receive encrypted information from a portable PCS device to a tactical user of the Mobile Subscriber System. Tactical PCS secures network data broadcast and multicast by having radio access points or cell sites made small and rugged enough to mount on vehicles that travel with the tactical users. For tactical missions that require data to be broadcast and multicast to users covering a large area, a UAV may be used to interconnect cell sites throughout the large area to keep the broadcast and multicast data secure. Figure 9-3 illustrates interconnecting cell sites using a UAV.



iatf\_9\_3\_0131

Figure 9-3. Interconnecting Cell Sites Using a UAV

## 9.7.4 Framework Guidance

Future tactical systems will demand the use of commercial equipment and infrastructure. Thus, interoperable signaling plans and protocols should be integrated throughout all tactical systems. The FNBDT is a network-independent, common cryptographic and signaling protocol that is implemented in CONDOR and the tactical STE. Inclusion of these protocols in systems such as the JTRS would dramatically improve interoperability, reducing the suite of duplicate systems a tactical user must carry.

Another technology gap involves the use of UAVs as an airborne communications node for tactical cellular. Current military UAVs, particularly the Global Hawk, Dark Star, and Predator systems, are used exclusively for aerial reconnaissance. Significant improvements in tactical C<sup>2</sup> would be possible by expanding the UAV mission to include its use as an ACN.

## 9.8 IA Solutions in Low Bandwidth Communications

One certainty of future tactical communications environments is that the warfighters on the battlefield at the lower levels of the command structure will continue to have smaller bandwidths and lower data rates available to them than the higher echelons. Also, the soldier on the ground or the pilot in the air has significantly less carrying capacity available for additional equipment than do fixed facility organizations. These constraints of bandwidth and lift are key drivers when implementing viable IA solutions at the tactical level.

The combination of limited funding for GOTS IA solutions and improvements in the strength of commercial solutions will lead to military systems of the future relying more on commercial IA tools to provide adequate security services. Unfortunately, IA technologies such as network monitoring systems occupy additional bandwidth that cannot be used for actual communications. To meet the objective of integrating IA solutions into the battlefield, these tools must operate with low bandwidth communications systems at the warfighter level without a noticeable degradation in the speed or accuracy of critical-mission data traffic.

### 9.8.1 Mission Need

DoD would like to implement commercial IA tools in its tactical communications systems to decrease costs while increasing security and interoperability with the sustaining base. However, current tactical systems are not equipped to handle these commercial tools. As reported recently in *Federal Computer Week*: “Tactical battlefield networks under development by the Army and Marines to support operations on future digitized battlefields have vulnerabilities,” according to ‘MG Robert Nabors, commander of the Army’s Communications-Electronics Command. “Army tactical battlefield networks,” Nabors said, “do not have the bandwidth to handle commercial [IA] tools.” [10] Furthermore, current planners estimate that the bandwidth available to the

## UNCLASSIFIED

Information Assurance for the Tactical Environment  
IATF Release 3.1—September 2002

tactical soldier will likely remain low (tens of kbps). Given these constrained bandwidths, tactical users cannot afford IA solutions that impose additional bandwidth demands. Therefore, there is a requirement to adapt current IA technologies to lower bandwidth applications.

IA solutions that require significant bandwidth are not likely to be employed in the bandwidth-constrained environment of tactical operations, leaving tactical units with no alternative but to continue to operate with low—or no—assurance solutions. Network monitoring systems and intrusion detection systems employed on a tactical communications network can be monitored from the main operating base, or other rear echelon location. However, these systems send monitoring data from the end-user equipment back to the monitoring station. Thus, valuable bandwidth is occupied by monitoring traffic, decreasing the amount of bandwidth available to the warfighter or other operator for vital mission data. Without these IA solutions, a unit's network traffic could be subject to undetected interception and decryption by adversaries, ultimately leading to mission failure and loss of lives.

### 9.8.2 Consolidated Requirements

- Tactical networks require implementation of low profile IA monitoring tools that use minimal network bandwidth.
- In the long term, tactical networks must increase available bandwidth from tens of kbps to tens of Mbps to handle sophisticated, commercial IA tools.

### 9.8.3 Technology Assessment

Legacy military communications and information systems have traditionally been “closed” systems, meaning that equipment is designed specifically for use in one system. This is in contrast to the current philosophy of migrating to an open systems architecture. In the past, low bandwidth communications used symmetric keying systems to provide confidentiality, and few network monitoring applications were available to ensure network security. Systems were not interoperable, and tactical forces learned to work around the constraints associated with closed systems. As communications and information systems move to an open systems environment, radios and networks from the fixed plant to the tactical domains must include a full suite of IA solutions to remain effective for military operations.

Remote network management plays a large part in maintaining the security of tactical networks. Using advanced network monitoring applications, a technical controller can remotely monitor the security of several deployed networks from a central location. Tactical equipment typically has less bandwidth and processor capacity than fixed plant equipment. Therefore, it is more difficult to implement commercial IA tools in tactical communications networks and equipment. Current battlefield networks do not have the bandwidth to handle commercial tools like network monitoring and intrusion detection tools. However, programs are under way that may make it easier to integrate commercial IA tools into tactical systems. Two major programs will benefit from this integration: the JTRS and the Marine Corps End-User Terminal (EUT).

**Note:** The Joint Tactical Radio program applies to several issues in this Framework. To avoid duplication of text throughout each issue, JTRS will be discussed exclusively in this section.

Joint Tactical Radio System (JTRS) will be the next-generation radio for U.S. military forces in the 21st Century. In a memorandum to the Service Acquisition Executives in August 1998, the Office of the Assistant Secretary of Defense for Command, Control, Communications and Intelligence (OASD C<sup>3</sup>I) suspended all other “efforts to initiate any contracting activity to develop and acquire any radio system to include software-programmable radio technology.” The JTRS Joint Program Office (JPO) is responsible for developing a family of JTRS products having common architecture and designed to serve different operational environments. As of this writing, the JTRS JPO was in the Phase 1 process of selecting the architecture to use for the production of the first JTRS prototypes (Phase 2). Therefore, specifics on JTRS will not be available until later revisions of this Framework.

JTRS will be a family of radios that provide simultaneous multiband, multimode, and multiple communications using existing and advanced data waveform capabilities to ensure the timely dissemination of battle space C4I and global navigation information. The JTRS software-defined radio design represents a significant paradigm shift merging the commercial computer and networking industries with the wireless communications industry. Although these technologies may prove beneficial in the commercial industry, implementing IA technologies into a Software Defined Radio (SDR) presents several new challenges. High-assurance software components must be developed and certified to perform in a manner acceptable for Type 1 security. A major benefit of JTRS is the scalability of the architecture. For a tactical unit, a handheld form factor should prove useful in satisfying the need for a low-bandwidth secure solution.

Overall, the benefits of JTRS significantly outweigh any technology issues that arise. Because the JTRS architecture is flexible and relies on many COTS products, a single Joint Tactical Radio can be scaled to meet the needs of any tactical unit. Airborne, vehicular, man-portable, and handheld versions will be available for use in the tactical arena, providing secure and nonsecure voice, video, and data communications using multiple narrowband and wideband waveforms. Operators will be able to load and/or reconfigure modes and capabilities of the radio while in the operational environment. Techniques such as OTAR, OTAZ, and other key management services are employed to overcome several of the IA issues discussed in this Tactical Framework. As this program develops, future versions of this Framework will address JTRS in more detail.

## **U.S. Marine Corps End User Terminal**

The EUT is a technology currently in the testing phase by the U.S. Marine Corps. The EUT provides low bandwidth, networked communications at the squad level. However, the system currently lacks available security solutions. During recent Urban Warrior exercises, the Marines tested an EUT vest, composed of a minilaptop computer running MS Windows, Netscape, and SRI's INCON Common Tactical Picture (CTP) software. These vests use differential Global Positioning System (GPS) for positioning and wireless Ethernet to communicate with one or more wireless access points. The mini-laptops have two PC card slots that are used by the

## UNCLASSIFIED

Information Assurance for the Tactical Environment  
IATF Release 3.1—September 2002

wireless LAN PC card and for cellular phone PC card adapters. Additionally, high-bandwidth wide area network (WAN) connectivity is provided to the CTP via Very Small Aperture Terminal (VSAT) SATCOM and/or leased T1 lines. Thus, all the squads of Marines can access the CTP, including video feeds, intelligence images, and real time-updates. The CTP is also available to helicopters, boat units, light armored vehicles, and reconnaissance forces in the tactical area.

To date, all the Marine Corps Urban Warrior exercises have been unclassified; thus, minimal work has been conducted regarding cryptographic and IA solutions to secure the EUT and CTP software. Early testing has focused on integrating commercial networking technologies onto the tactical battlefield. Future solutions will likely employ some of the same high-assurance software products under development for the JTRS program. For additional information about commercial wireless LAN technologies, refer to the IATF Section 5.2.3, Wireless LAN.

### 9.8.4 Framework Guidance

Tactical users are encouraged to implement network monitoring, intrusion detection, and other IA tools in battlefield and other tactical environment networks. The adversaries of tomorrow will have the network savvy required to attack tactical networks. Detection and prevention of network intrusions will go a long way to insure the security of sensitive communications. Meanwhile, this Framework encourages the development of higher data rate (100s of Mbps) systems available at the lowest warfighter level with enough processing power to implement COTS security solutions in a handheld and man-portable form factor.

## 9.9 Split-Base Operations

Split base refers to a situation in which a unit deploys from its home base to a forward-operating base in or near the battlefield. As the United States decreases the permanent presence of its military forces on foreign soil, the number of such split-base operations will continue to increase. In forward operations, it is preferable to bring along as little infrastructure as possible. The goal is to maximize forward capability. One approach is to leave infrastructure “at home” and rely on communications links to tie the warfighter at the front to the infrastructure at home. However, units must retain the capability to deploy to any site worldwide, bringing an entire suite of equipment to the battlefield that can operate securely, without relying on specific IA tools available at that site. Although the proximity to the battlefield may vary according to the service in question (e.g., Air Force versus Army units), the IA issues relating to split-base operations will generally remain the same. IA concerns for split-base operations actually incorporate several other issues already discussed in this tactical section. However, specific IA issues relating to split-base operations are discussed here because of the importance of secure communications during these types of operations.

To better support split-base operations, the services have programs in place to upgrade the communications infrastructure of military installations worldwide. DoD has embraced the idea

## UNCLASSIFIED

Information Assurance for the Tactical Environment  
IATF Release 3.1—September 2002

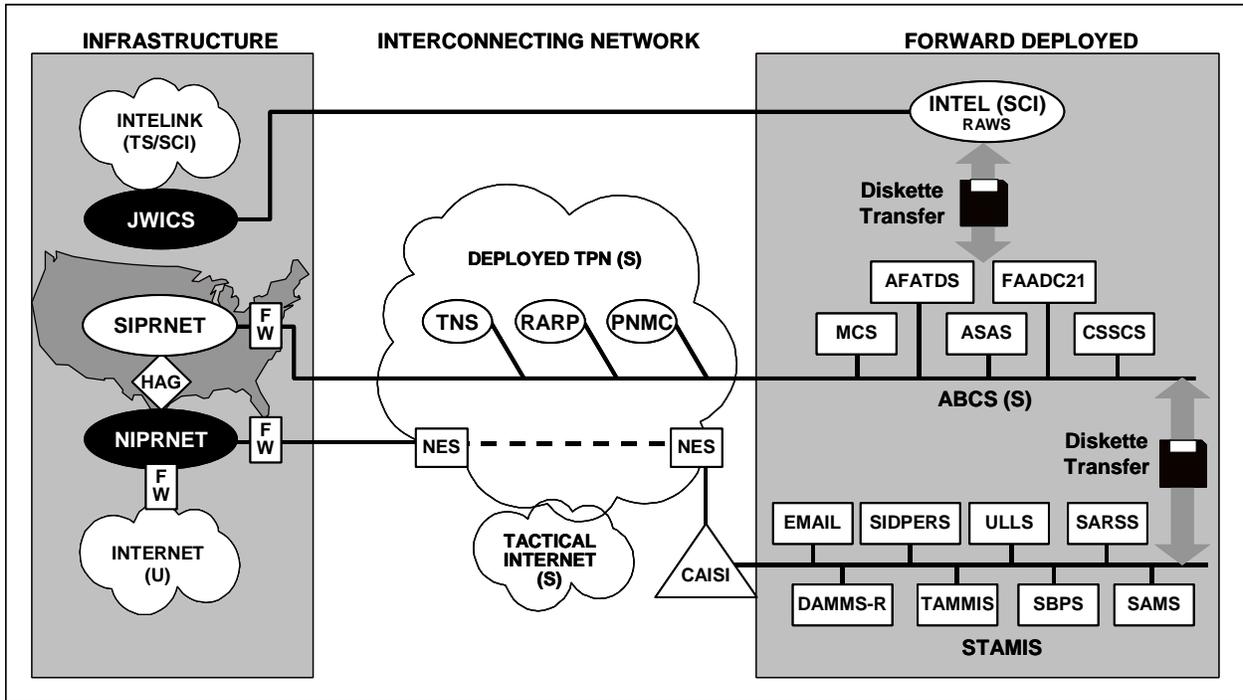
of “network-centric warfare,” where tactical, logistics, and intelligence information becomes as much a weapon for the warfighter as firepower. Joint Vision 2010 puts networks at the center of military strategy for the next decade. Each service has separate programs in place to upgrade and standardize the client/server-based local, metropolitan, and WANs throughout the DoD. These programs are discussed below in the technology assessment area.

Infrastructure upgrades will drastically improve the support for deployed tactical forces, providing the capability to transport high-volume, real-time  $C^2$ , and intelligence data to support contingency deployments and split-base operations during peacetime and war. As a rule of thumb, when a unit (or part of a unit) deploys to a forward area, an immediate demand exists for secure, high-capacity communications back to the main base. Today, most Air Force squadrons will deploy to an existing airbase near the theater of operations where communications capabilities are already in place. However, this is not always the case for tactical ground forces. When a tactical Army unit deploys to an area that does not have an existing communications capability, technologies must be available to enable the rapid setup of secure voice, data, and video communications systems, linking the deployed unit to the home infrastructure. As the networking infrastructure of U.S. bases improves, tactical units must have the capability to connect securely back to their home networks. Tactical forces will likely rely heavily on SATCOM and other wideband systems to provide these secure communications between home base and the TPN forward.

An example from the WIN Master Plan is used to illustrate the split-base operation concept. Today’s equipment does not provide for multilevel security over a single channel. Current security policy for the TPN mandates that all hardware be accredited for secret high operation. (The exception to this policy is the tunneling of Unclassified but Controlled Standard Army Management Information System (STAMIS) users via in-line network encryption (currently, the Network Encryption Systems [NES]) through the deployed TPN. For specific guidance on tunneling of lower classification data over a classified system-high network, refer to Section 5.3.7 in System High Interconnects and VPNs.

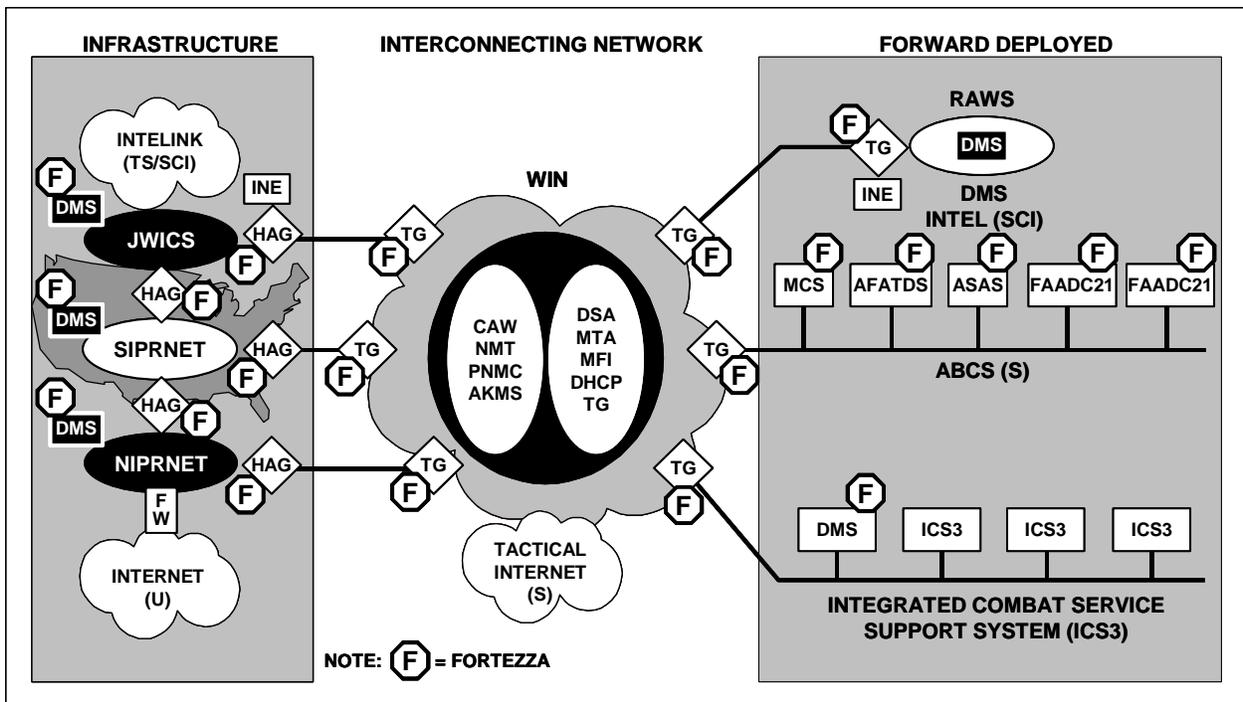
Today’s typical configuration, shown in Figure 9-4 taken from the WIN, calls for the use of firewalls at gateway points between network types and High Assurance Guards (HAG) between the Secret Internet Protocol Router Network (SIPRNET) and Nonclassified Internet Protocol Router Network (NIPRNET). Figure 9-5 illustrates the objective configuration implementing

MLS with FORTEZZA<sup>®</sup> or other programmable cryptography at each node. Tactical forces that connect to the TPN need the ability to wirelessly pull information from SIPRNET, NIPRNET, or the Joint Worldwide Intelligence Communications System (JWICS) databases from their deployed location. Improvements to the network infrastructure will improve  $C^2$  in split-base operations. Furthermore, security services such as confidentiality, data integrity, and access control mechanisms become increasingly important for a commander communicating with forward-deployed tactical forces. These services must continue to be a part of the TPN infrastructure.



iatf\_9\_4\_0132

Figure 9-4. Near-Term Architecture [11]



iatf\_9\_5\_0133

Figure 9-5. Objective WIN Security Architecture [11]

As stated previously, many of the IA issues discussed elsewhere in this chapter are particularly applicable to split-base operations.

## 9.9.1 Mission Need

Split-base operations are a culmination of all the tactical IA issues described in this Framework. Each IA issue must be addressed to securely execute the split-base operations described in the WIN and other Joint Vision 2010 documents. Furthermore, as the number of permanent U.S. overseas installations decreases, the separation between “home” and “forward” will more and more often be between CONUS and “forward.” Network technology must provide a robust multimedia, theater-level communications networking infrastructure that can be rapidly deployed to support tactical operations. Several security implications are associated with maintaining communications links between the home base and a deployed location.

As an example, all types of information, from logistical supply data to intelligence data, traverses the communications link between the deployed location and the home base. For a sophisticated adversary with access to transcontinental communications, eavesdropping, disrupting, or denying the communications links necessary for successful split-base operations can give an adversary a significant military advantage.

## 9.9.2 Consolidated Requirements

The goal of a successful split-base operation is to maximize forward capability, while minimizing the amount of infrastructure required at the forward location. Thus, in addition to the requirements listed in the previous sections, the following requirements exist for IA in a tactical split-base operation:

- Infrastructure upgrades must occur in home-base networks to improve the support for deployed tactical forces. These upgrades must provide the capability to transport high-volume, real-time C2, and intelligence data such as battlefield video teleconferencing and transfer of satellite imagery to forward units.
- Tactical units must bring a suite of equipment to the battlefield that can be securely configured at any site, without relying on IA solutions available at that site.
- Technologies must be available to the warfighter at forward locations to enable rapid setup of secure voice, data, and video communications systems.
- IA technologies must be in place to prevent a sophisticated adversary from eavesdropping, disrupting, or denying the communications links necessary for successful split base operations. Proper implementation of security solutions discussed in Chapters 5 through 8 of this IATF can provide adequate protection for a split-base operation.

## 9.9.3 Technology Assessment

Well coordinated split-base operations require a sophisticated communications infrastructure at the base level in the CONUS. Based on guidance from Joint Vision 2010, the services have kicked off several programs aimed at improving this infrastructure at the base level. These programs are discussed below.

The Navy has the Information Technology for the 21st Century (IT-21), which defines a standard, networked computing environment, based on commercial technology, for its ashore and afloat units. Key Army initiatives include the Outside Cable Rehabilitation (OSCAR) program, Common User Installation Transport Network (CUITN), Army's DISN Router Program (ADRP), and Digital Switched Systems Modernization Program (DSSMP). These programs will update the Information Technology (IT) infrastructure at Army facilities in the United States, providing an all-fiber ATM network to support real-time wideband data requirements like video teleconferencing. Finally, the Air Force is implementing a base-level Combat Information Transport System (CITS) that includes installation of fiber-optic cable, ATM switches, hubs, and routers at 108 bases. As a vital part of CITS, information protection hardware and software will be installed as part of an Air Force standard network management system.

### **Theater Deployable Communications Integrated Communications Access Package Program: Rapid Communications Setup in a Drop-in Airbase**

The U.S. Air Force also has contracted to develop a new advanced rapid deployment communications network to be used to deploy critical communications assets at a "drop-in" airbase. The program, called the Theater Deployable Communications Integrated Communications Access Package Program (TDC-ICAP), will provide secure and nonsecure voice, data traffic for local area, intra-theater, and intertheater communications using commercial components. The deployment of the TDC-ICAP will enable all of the U.S. Air Force elements (command and control, intelligence, logistics, and mission support functions) to function in a coordinated manner from initial deployment through sustainment.

The TDC provides a ground-to-ground communications infrastructure designed to transmit and receive voice, data, and video communications securely to or from wireless, satellite, or hard-wired sources. This modular and mobile system will allow the Air Force to tailor the system to its specific needs and to transport the system anywhere worldwide. Thus, TDC-ICAP drastically reduces the communications problems typically associated with airlift and manpower. The system is configured into common man-transportable transit cases to optimize airlift capability and to ease the problem of ground deployment.

TDC-ICAP interfaces with legacy TRI-TAC equipment through an adaptation of existing SMART-T technology developed for the Milstar system. Additionally, the ICAP is compatible with the telephone systems in 39 countries wide, providing connectivity through a commercial

Private Branch eXchange (PBX) to the local phone system. The center of the TDC-ICAP complex is the base hub, which supports all users located at its specific location. Additionally, all off-base communication passes through the base hub for distribution and is handled by the off-base hub for specific interfaces, bulk encryption and decryption, and multiplexing.

The TDC-ICAP provides secure, tactical communications services to forward-deployed Air Force units virtually anywhere worldwide. Rapid deployment of a core communications capability is central to the success of this program. Core communications can be set up in 1.5 hours after the initial pallets of equipment are delivered on site. Access is provided for TRI-TAC KY-68 encryptors. Two-wire and Integrated Services Digital Network (ISDN) interfaces are available at all nodes in the system allowing connection of STU-III or STE terminals for secure voice and secure fax capabilities. In addition, it is designed for transition to Defense Message System (DMS) compatibility, when that system is phased in. [12]

## 9.9.4 Framework Guidance

Split base operations will continue to present new technological challenges to the tactical unit commander. As the communications infrastructure improves, the forward commander will have access to increased bandwidth and unparalleled connectivity to rear-echelon networks. Tactical units will be able to access the NIPRNET and SIPRNET from their forward locations. One key technology gap identified in this framework involves pulling information from the SIPRNET over a wireless link. A commercial PDA user can pull a map off the Internet, get directions, or access a database at the office from virtually anywhere in the country. However, a soldier on the battlefield has no way to access the SIPRNET to pull down a classified map or view overhead imagery. Continued developments in JTRS may help resolve this issue.

## 9.10 Multi-Level Security

As the U.S. military and other agencies with tactical missions move toward the next generation of radios and communications equipment, MLS has become an increasingly important technology hurdle. MLS implies a communications device that can simultaneously process data communications at different levels of classification. A radio on an unclassified network (e.g., HaveQuick in an Air Force network) will need to communicate with both unclassified networks and data systems in a tactical Internet operating at the secret-high level. Interoperability—the exchange of data between different classification levels—has become a necessity. As a result, MLS solutions are needed to integrate the majority of individual military communications systems into an interoperable ensemble of capability. Because of the difficulty involved with fielding a true MLS solution, this section focuses on MLS more as an objective than a requirement.

Traditional security policies mandate strict physical separation of systems and data at different classification levels. However, as the military moves toward a Software Defined Radio (SDR), physical separation is difficult, if not impossible, to achieve. MLS solutions will integrate high-

assurance hardware and high-assurance software solutions, eliminating the need for separate COMSEC devices and red processors at each independent classification level. Integrated MLS solutions yield critical size, weight, and power reductions, lightening the load for a tactical warfighter.

A cornerstone of multi-level security solutions is programmable cryptography. Programmable cryptography is a set of hardware and software capable of changing COMSEC algorithms and keys, allowing one device to interoperate with several different COMSEC devices. Current legacy communications equipment typically uses a COMSEC device particular to that equipment or to the specific channel on which a radio is operating using one COMSEC algorithm at a time. In contrast, programmable cryptography enables communications equipment to load several different COMSEC keys simultaneously, allowing a single radio to “talk” on several different nets without requiring separate COMSEC devices or having to reload COMSEC for each net. In addition, new algorithms can be added via secure software, and old ones can be deleted. Last, upgrades to programmable cryptographic devices are done in software, instead of hardware board replacements of legacy COMSEC equipment. This issue corresponds to Section 9.2, Wiping Classified Data From Tactical Equipment.

## 9.10.1 Mission Need

True multi-level security solutions (at Type 1 security levels) have never been achieved for tactical systems. Communications at different security levels remains a complicated challenge. Separate red processors are required not only at each classification level, but also at separate buses and red devices for each level. Unfortunately for the tactical warfighter, this means more equipment in the field. A transition must be made from secret-high operations to Multiple Independent Security Levels (MILS), and eventually to true multi-level security through the use of programmable cryptography.

A true MLS solution, as proposed in JTRS, would implement a programmable cryptographic chip in a single radio. Several different levels of cryptographic key would be loaded in the same chip, allowing the airborne troops to carry only a single radio into battle, freeing part of their limited load for other items, such as ammunition. Use of programmable cryptography for MLS will increase interoperability between networks at different levels and will decrease critical equipment requirements for the warfighter.

## 9.10.2 Consolidated Requirements

- Multi-level security solutions are needed to integrate the majority of individual military communications systems—increasing interoperability and reducing critical size, weight, and power requirements for the tactical user.
- A transition must be made from secret-high operations to MILS, and eventually to true multi-level security through the use of programmable cryptography.

- Programmable cryptographic solutions used in concert with trusted OS must be available in the future enabling tactical communications systems to enable multiple levels of classified information on a single radio.

## 9.10.3 Technology Assessment

Multi-level security solutions will eventually be implemented in hardware or software or a combination of both. A hardware approach relies on physical separation of data at different classification levels, and it can be difficult to upgrade if modifications become necessary. However, by using a hardware-software combination solution, the hardware effects can be minimized. Hardware elements such as programmable cryptography can be used to eliminate the need for separate COMSEC devices and Red processors at each classification level. Part of this section briefly discusses some of the programmable cryptography programs under development.

In addition, a hardware-software combination MLS design may include use of a trusted OS, coupled with a trusted middleware solution. A high-assurance, software-based data control scheme ensures data separation for different classification levels. The advantages of this type of implementation are flexibility, portability, and minimal hardware dependency. Also, new security technologies can easily be added through software upgrades. A large number of real-time OSs are available. The choice of which OS to use for a particular application should be made judiciously, considering such issues as interoperability and performance parameters. Systems such as JTRS require Portable OS Interface Unix (POSIX) (IEEE 1003) compliance for the OS.

Several major programmable cryptography programs are under way, including AIM, Cornfield, FORTEZZA<sup>®</sup> Plus, Cypris, and the Navy's Programmable Embedded INFOSEC Program (PEIP). Certain devices fit better in different form factors, and allow several channels to operate simultaneously. Specific solutions should be chosen judiciously on a case-by-case basis. This section is not intended to cover each program in detail or to recommend a specific device. Rather, to increase equipment interoperability and decrease the amount of COMSEC equipment required in the field, this Framework encourages continued improvements to current programmable cryptographic devices.

Programmable cryptography on embedded cryptographic chips will help pave the way to achieving full multi-level security solutions. Refer to the earlier discussion about JTRS for an example of a future tactical application of MLS. Programmable cryptography relies on high-assurance components that perform the function of maintaining separation of data at different classification levels. Instead of physical separation, these devices maintain strict data separation within the chip. Successful implementation of these chips in tactical communications equipment will reduce the amount of equipment required in the field and will reduce the number of COMSEC keys and equipment to be maintained in a hostile environment. Coupled with proper media encryption and zeroizing technologies, a true multi-level security solution will significantly enhance the effectiveness of tactical communications.

## 9.10.4 Framework Guidance

True multi-level security solutions do not exist. This Framework encourages continued research in programmable cryptography and in the development of trusted OS, to approach true MLS implementation. The JTRS program has a requirement for MLS operation three to six years down the road. Until then, systems will operate with MILS. As a stepping stone toward MLS, MILS implies multiple classification levels of data in the same system as separate channels. Until true MLS is achieved, tactical units should implement MILS systems and components wherever possible to lighten the equipment load on the warfighter.

## 9.11 Additional Technologies

Given the format of this chapter, certain tactical systems that will play key roles in future tactical communications did not seem to fit any of the specific categories discussed above. Therefore, these systems are discussed here: Tactical STE (TAC/STE), ISYSCON, and Battlefield Video Teleconferencing (BVTC).

### Tactical Secure Telephone Equipment

STE is the next generation of secure voice and data equipment for advanced digital communications networks. The STE consists of a host terminal and a removable security core. The host terminal provides the application hardware and software. The security core is a FORTEZZA<sup>®</sup> Plus Krypton cryptographic card, which provides all the encryption and other security services. The STE is available in two models: Office STE and Tactical STE.

The TAC/STE provides secure tactical and strategic digital multimedia communications, interoperating with legacy TRI-TAC equipment, while also providing basic ISDN and STU-III compatibility in a single unit. The TAC/STE provides direct connection to tactical communication systems in the field and offers full office features and connectivity for use in garrison. The design is based on the open, modular architecture, allowing efficient software upgrades to deployed units. TAC/STE is TRI-TAC/MSE Interoperable and supports 16/32 kbps CVSD clear secure operation via LPC/CELP. In addition, the Tactical STE PCMCIA Cryptography uses a removable FORTEZZA<sup>®</sup> Plus Krypton Card that supports Unclassified but Controlled through Top Secret/Sensitive Compartmented Information (TS/SCI) traffic. For more TAC/STE information, visit <http://ste.securephone.net/>. [13]

### ISYSCON

Any tactical force deployment will require a number of communications networks. MSE, the mainstay for tactical area communications, operates alongside TRI-TAC assemblages. A vital flow of information gathered by the Joint Tactical Information Distribution System (JTIDS) is simultaneously relayed throughout the battlefield for air defense. Enclaves of soldiers will respond to urgent information passed over their combat net radios (CNR). The EPLRS constantly updates and transmits its location information. The complexity and magnitude of these communications networks demand a means of integrating systems control to maximize the

effectiveness and availability of the various systems and to ensure their interoperability. The ISYSCON program provides this tactical area communications management capability.

The ISYSCON program brings a higher level of integrated communications management to theater tactical communications through a common mechanism, complete with automated tools, to seamlessly integrate communications systems at all levels. ISYSCON optimizes the application of standard Army Frequency Management, COMSEC, and Communications-Electronics Operating Instruction (CEOI) modules; provides automatic interfaces to the Battlefield Functional Area Control System (BFACS); and incorporates unique decision aides and embedded training capabilities.

In the near future, joint communications planning and management for regional Commander in Chief (CINCs) and joint forces commanders will be provided by the emerging Joint Network Management System (JNMS). JNMS will facilitate communications network engineering, monitoring, control, and reconfiguration. It also will perform frequency spectrum management and IA management.

## **Battlefield Video Teleconferencing**

Faster processor speeds and improved modulation techniques have boosted the commercial use of VTC dramatically in recent years. Naturally, the desire to make use of this capability has transferred to the tactical battlefield. The BVTC is a state-of-the-art, near full-motion interactive VTC system that enhances coordination and provides an additional combat multiplier to the warfighter. This technology can be applied at many levels through the battlefield. Two areas that will likely see great enhancements by the use of BVTC are warfighter C<sup>2</sup> and telemedicine.

BVTC enhances C<sup>2</sup> by allowing the warfighter to effectively disseminate orders, clearly stating intent. The warfighter can conduct collaborative planning and whiteboarding with subordinate commanders and key staff elements. (See Figure 9-6.)

Medical units are supported by telemedicine from remote deployment areas, where skeletal medical forces receive assistance from specialists at sustaining-base hospitals. Other applications exist at several regional medical centers (Tripler, Walter Reed, and Landstuhl) to provide specialized diagnosis and care to remote medical facilities. Telemedicine will project the valuable expertise and skills of rear-based specialists to forward-deployed medics.

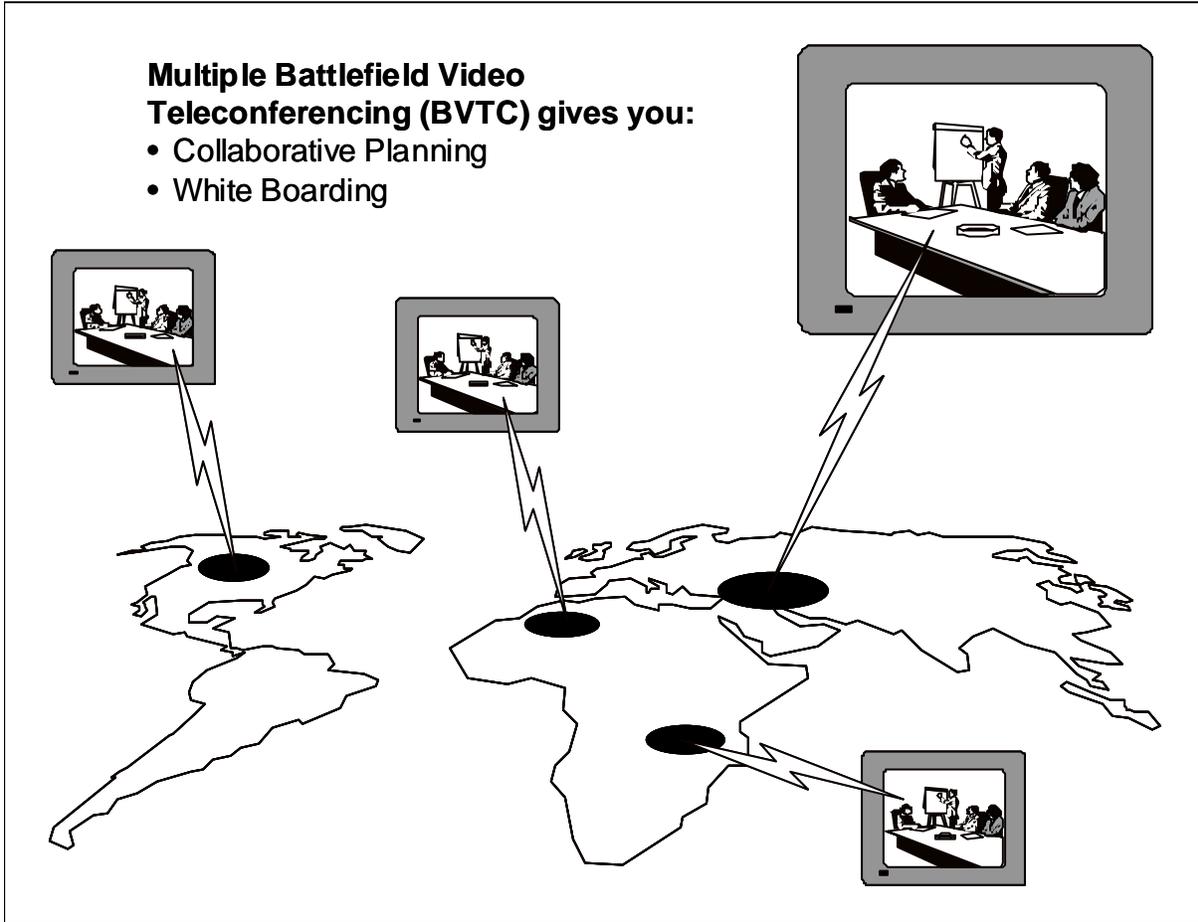
Commercial development of VTC should drive the development of faster, highly capable network VTC applications. With the addition of data integrity and confidentiality mechanisms, VTC should transfer well to tactical applications. The wide bandwidth signals used with BVTC will require high-speed cryptographic solutions. A high-tech adversary could gain battle damage assessment or other sensitive information simply by intercepting a telemedicine BVTC channel. The development of high-speed, reprogrammable cryptography will speed the implementation of the necessary INFOSEC solutions to BVTC.

BVTC components (e.g., cameras, monitors, computers, microphones) are user owned and operated. The features and capabilities employed at each echelon or activity will be based on the

**UNCLASSIFIED**

Information Assurance for the Tactical Environment  
IATF Release 3.1—September 2002

requirements of that specific echelon or activity. The Army's WIN architecture will provide the bandwidth and throughput required to support BVTC for both point-to-point and multipoint conferencing. BVTC capability will be provided to users of the WIN with nominal impact on the remainder of the network.



iatf\_9\_6\_0134

**Figure 9-6. Battlefield Video Teleconference**

## UNCLASSIFIED

Information Assurance for the Tactical Environment  
IATF Release 3.1—September 2002

### References

1. Mobile Ad-hoc Networks (MANET) Web Page, <http://www.ietf.org/html.charters/manet-charter.html>.
2. Mobile Ad Hoc Networking Working Group Web Page, <http://www.ietf.org/rfc/rfc2501.txt>.
3. Hewlett Packard Web Site, [http://www.hpl.hp.com/personal/Jean\\_Tourrilhes/MobileIP/](http://www.hpl.hp.com/personal/Jean_Tourrilhes/MobileIP/).
4. BBN Technologies Web Site, <http://www.net-tech.bbn.com>.
5. Deputy Secretary of Defense Memorandum, Department of Defense (DoD) Public Key Infrastructure (PKI), May 6, 1999.
6. DFAS PKI Study, March 10, 1999, <http://www.gradkell.com/PKI/DfasPkiStudy/DfasPkiStudy.PDF>.
7. Condor Wireless Security Web Site, August 9, 2000, <http://condor.securephone.net>.
8. Defense Advanced Research Projects Agency (DARPA) Web Site, August 1, 2000, <http://www.darpa.mil>.
9. Reserved.
10. Brewin, Robert and Daniel Verton. "DoD Leaders Mull Internet Disconnect." *Federal Computer Week*, April 19, 1999.
11. Warfighter Information Network Master Plan, Version 3. 3, June 1997.
12. Motorola Web Site <http://www.mot.com/GSS/SSTG/ISD/ic/TDC.html>.
13. Secure Terminal Equipment (STE) Web Site, August 10, 2000, <http://ste.securephone.net/>.

### Additional References

- a. Network Security Framework, Version 1.1. December 3, 1998.
- b. Shalikashvili, Gen John M. Joint Vision 2010. Joint Chief of Staff: Washington DC, July 1996.
- c. United States Army Communications-Electronics Command. CECOM Vision 2010. New Jersey, 1997.
- d. JBC Information Assurance (IA) Tools for the Joint Task Force (JTF) Phase III Assessment Quicklook Report Summary. February 1999.
- e. Linton, Dennie. Global Broadcast Service: Shrinking the Year-2000 Battlefield by Spreading the Word (Globally).
- f. Fillgrove, Ted. "Update on Enhanced Position-Location Reporting System."
- g. Newton, Harry. Newton's Telecom Dictionary. Telecom Books, October 1998.

## UNCLASSIFIED

Information Assurance for the Tactical Environment  
IATF Release 3.1—September 2002

- h. Marine Corps Operation Urban Warrior Web Page,  
<http://www.defenselink.mil/specials/urbanwarrior/>.
- i. SRI International InCON Web page, <http://www.sri.com/news/releases/05-07-01.html>.