Chapter 3

Land Information Warfare Activity (LIWA)

Introduction

The Land Information Warfare Activity (LIWA), a Headquarters Department of the Army operations support activity assigned to the Intelligence and Security Command (INSCOM), provides multi-discipline Information Operations (IO) support to the U.S. Army's component and major commands. LIWA has broad authority to coordinate IO topics and establish contact with Army organizations, USN, USAF, and JCS IO Centers, and with DoD and National Agency IO elements.

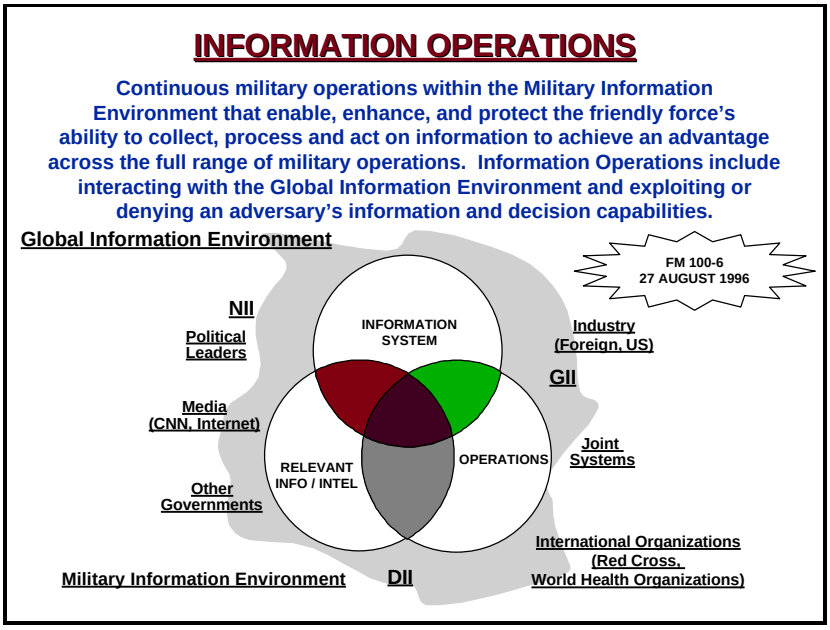

Figure 3-1, Information Operations

> LIWA has broad authority to coordinate IO topics and establish contact with Army organizations, USN, USAF, and JCS IO Centers, and with DoD and National Agency IO elements.

Figure 3-2 graphically portrays the commands, agencies and organizations LIWA routinely coordinates with to support IO planning, and operations. The oval in the center represents LIWA, the circles on the perimeter of the oval depict the organizations LIWA coordinates with as it provides IO support to the field. LIWA also interfaces with the other organizations shown on a

frequent and continuing basis to deal with issues related to policy, programs, concepts, doctrine, IO planning, and operational support.

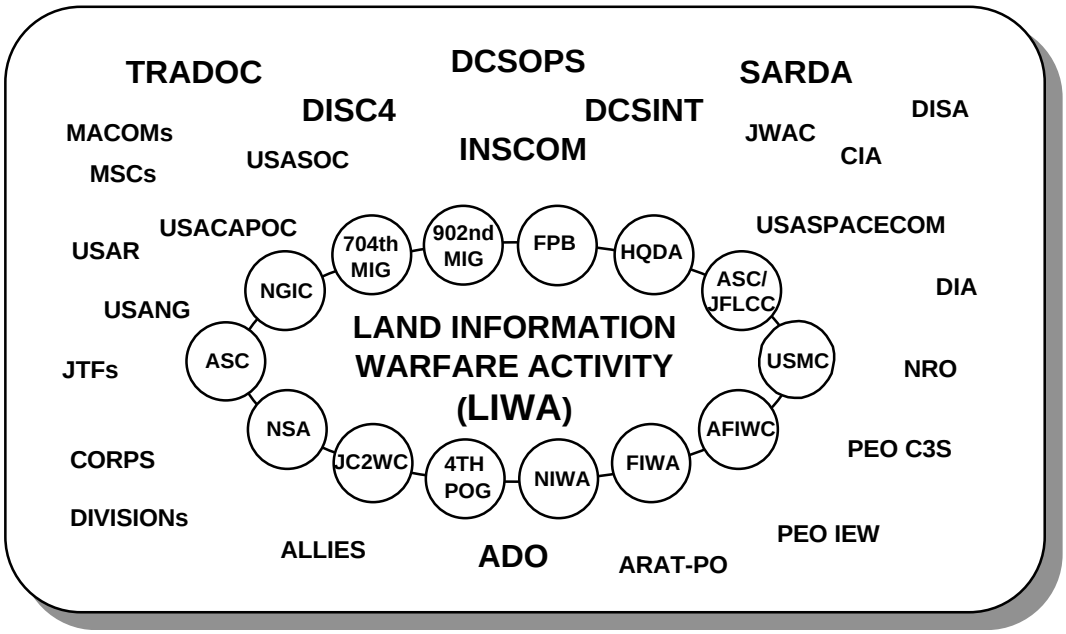

Figure 3-2, LIWA Relationships

IO Strategic Role

The ***strategic goal*** of IO is to promote freedom of action for U.S. Forces while hindering adversary efforts. U.S. Army IO integrate all aspects of information to support and enhance the elements of combat power, with the goal of dominating the battle space at the right time, at the right place, and with the right weapons or resources. Activities to support IO include acquiring, using, protecting, managing, exploiting, and denying information and information systems. The ***strategic purpose*** of IO is to secure peacetime national security objectives, deter conflict, protect DoD information and information systems, and to shape the information environment. If deterrence fails, IO seeks to achieve U.S. information dominance in order to attain specific objectives against potential adversaries in time of crisis or conflict. Information Operations focus on maximizing friendly information capabilities, while degrading the opponent's information capabilities.

Army component commands may perform strategic missions such as employment of deep strike weapons, special forces, and other special capabilities. Information operations broadens the scope of strategic and EAC military operations. Emerging high technology military capabilities may be employed independently as stand-alone actions supporting national security objectives. When these capabilities are employed in a military operation they become part of the IO planning strategy under the control of a Unified or Joint Task Force (JTF) commander. Coordination with U.S. Army intelligence and operational threat analysis activities is essential for IO planning and operations.

Coordination with U.S. Army intelligence and operational threat analysis activities is essential for IO planning and operations.

Operational commanders weigh the advantages to be gained by countering adversary C2 nodes against the potential loss of intelligence from enemy signatures, radiation, or emissions, and the need to to protect intelligence sources and methods. In some cases, the decision authority to destroy or degrade an adversary's higher command echelons will be held at the national strategic level. Assistance in understanding an adversary's information system and his cycle of information processing is available through the Defense Intelligence Agency's (DIA) Tailored Analytical Intelligence Support to Individual Projects (TASIP).

The U.S. Army may be called upon to assist with Information Operations of another services, joint commands, National agencies, or allied forces as authorized by CJCSI 3210.01, DoD 3600.1, and AR 525-20. The U.S. Army could be assigned a specific IO mission by the National Command Authority (NCA), through the National Military Command Authority (NMCA), to an Army component of a unified command. The Joint term IW connotes the application of C2-Attack means to degrade or destroy an adversary's information system and to protect friendly command and control. Information Operations, unlike Information Warfare, are conducted continuously, e.g. defensive IO measures are applied routinely on a day-to-day basis. As a subset of IO, C2W is the application of IO strategy during military operations by engaging specific C2 targets. C2-Attack calls for the coordinated employment of destruction, deception, operations security, psychological warfare and electronic warfare, synchronized with the main operation.

The LIWA IO Role

LIWA teams support the Army Commander's goal of achieving Information dominance with the other JTF components or organizations. LIWA's purpose is to provide Army commands with technical expertise that is not resident on the command's general or special staff, and to exercise technical interfaces with other commands, service components, and National, DoD, and joint information centers. When deployed, LIWA FSTs become an integral part of the command's IO staff. To facilitate planning and execution of IO, LIWA provides IO/C2W operational support to land component and separate Army commands, and reserve components commands as required.

LIWA Mission

The mission of the LIWA is to provide IW/IO support to the land component and major/ separate Army commands, active and reserve component (AC/RC), to facilitate planning and execution of information operations (IO).

LIWA Functions

- Act as the focal point for Land IO.

- Coordinate, arrange for, and synchronize intelligence and counterintelligence support.
- Coordinate and deploy field support teams (FST) to assist and support the land component commands in C2-Protect and C2-Attack.
- Coordinate and deploy FSTs to provide battlefield deception support.
- Coordinate and assist TRADOC in the development and integration of doctrine, training, leader development, organization, materiel, and soldier requirements for IO.
- Act as the combat developer for C2-Attack and C2-Protect systems.
- Develop IO models and simulations in support of IO systems development, planning, training, and exercises.
- Assist in the development and integration of IO requirements in Army modernization strategy and policy scenarios, modeling, and simulations.
- Initiate and coordinate requirements for IO area studies.
- Assist in the development and evaluation of IO systems performance and operational employment tactics, techniques, and procedures in combat operations, operational tests, and training exercises.
- Identify technology for possible application to Army IO.
- Establish, develop, and promote IO interoperability with other services and allies.
- Assess IO force readiness and IO operational capabilities.
- Conduct IO vulnerability analyses of Army commands.
- Develop and sustain a rapid response capability to combat attempted penetrations of Army C2 systems and processes.
- Develop and coordinate requirements for operational IO from National and Defense reconnaissance.
- Identify and report changes in worldwide signature information that may require the software rapid reprogramming of Army Target Sensing Systems (ATSS), i.e., smart/brilliant munitions, sensors, processors, and aviation electronic combat survivability equipment.

Organization and Tasks

LIWA's functional support structure is shown in Figure 3-3, followed by a descriptive statement of the tasks and functions assigned to each LIWA component.

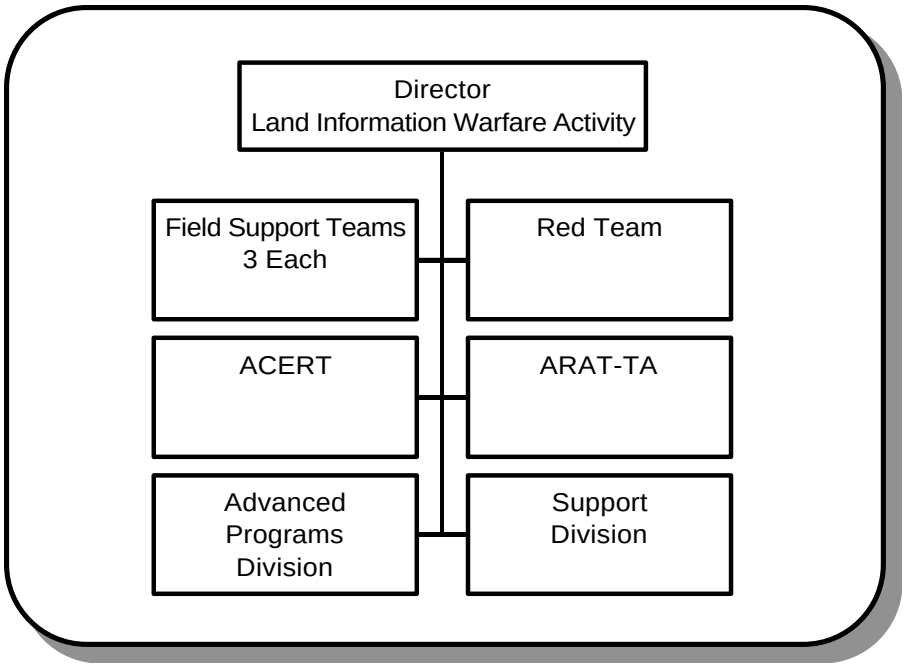

Figure 3-3, Major Functional Support Structure within LIWA

Office of the Director

Directs, controls, and coordinates all Information Operations activities in support of National, land component, and separate Army commands, active and reserve component, and interfaces with other IO/IW commands, activities, and agencies. Positions liaison personnel with selected agencies and IO centers.

Field Support Teams

Field Support Teams (FST) normally augment the Army or Land Component Command with IO expertise similar to the way JC2WC teams support the JTF or CINC.[1] FST will also support Army divisions and corps when needed to plan and implement information operations below the Army component command level. Team members consist of a need-driven mix of PSYOP, deception, OPSEC, EW, C2-Protect, C2-Attack, and intelligence specialties. When deployed, the FST becomes an integral part of the supported command's IO cell. The FST is structured to fill gaps in the command's IO cell, provide connectivity to CONUS resident agencies and databases supporting IO, and coordinate with the IO cells at the JTF or CINC level, as well as with the IW staff elements from other component commands in the operational area.

[1] **The Joint Command and Control Warfare Center (JC2WC), under the operational control of the JCS, provides the combatant commands and JTFs teams of command and control warfare specialists. Each JC2WC team has a habitual relationship with a supported command. Teams provide technical and operational specialists to support IO planning, operations, and exercises. The JC2WC emerged from the former Joint Electronic Warfare Center (JEWC), transitioning from purely EW to encompass all elements of C2W.**

The FST is structured to fill gaps in the command's IO cell, provide connectivity to CONUS resident agencies and databases supporting IO, and coordinate with the IO cells at the JTF or CINC level, as well as with the IW staff elements from other component commands in the operational area.

FSTs will be deployed to support operations ranging from peace keeping to major regional conflicts. FSTs also support operational planning, wargames, exercises, and training programs.

Red Team

The LIWA Red Team provides an Information Operations Vulnerability Assessment capability and an independent opposing force (OPFOR) type of capability to the Army component commands, the Army acquisition community, and separate Army commands. The Red Team provides a capability to assess the vulnerability of U.S. information, information systems, and information infrastructure.

- IOVAP: The Information Operations Vulnerability Assessments Program (IOVAP) provides the supported command a perspective of the command's susceptibility to an opponent's C2W operations. The IOVAP can be focused on garrison activities, field exercises, or both. In addition to isolating a command's vulnerabilities, the team recommends ways to reduce those vulnerabilities, allowing commanders to apply remedial action on the spot. In addition, the team will provide limited training to system managers on protection tools and procedures.

- OPFOR: The Red Team has the capability of assembling an independent C2W opposing force (OPFOR) to support exercises, and experiments. The size and composition of the OPFOR will vary by type of exercise, and by what must be learned about the command's vulnerability. Army warfighting experiments (AWE) involving brigade or division size elements may require high-technology intelligence systems and processors from the National level down to tactical Army systems, as well as systems from other services and agencies to provide the high-resolution information required. Other IO OPFOR operations may be successfully conducted using local collection systems.

Army Computer Emergency Response Team (ACERT)

ACERT's mission is to conduct Command and Control Protect (C2-Protect) operations in support of Army commanders worldwide. The objective is to ensure the availability, integrity and confidentiality of the information and information systems used in planning, coordinating, directing and controlling forces. ACERT supports systems administrators reporting suspicious activity on their computer networks. ACERT also has the responsibility of keeping Army leadership informed of incidents, and promulgating alerts and warnings based on information collected from a variety of sources.

Army Reprogramming and Analysis Team-Threat Analysis (ARAT-TA)

The ARAT-TA, supports warfighters, the commodity commands' post-deployment software support (PDSS) centers, and combat and materiel developers. ARAT-TA identifies and reports

changes in worldwide signature information requiring reprogramming of Army Target Sensing Systems (ATSS) software. Army Target Sensing Systems include smart and brilliant munitions, sensors, processors and aviation electronic combat survivability equipment. Identified threat signature changes are "flashed" to tactical units' subscribers over the ARAT Project Office electronic bulletin board.[2]

Advanced Programs Division

The Advanced Programs Division leads LIWA in the innovation, development, and employment of advanced IO/C2W capabilities (C2-Protect and C2-Attack) using multi-disciplined approaches. The Division monitors technology advancements, looking for opportunities to advance the state of the art in C2-Attack and C2-Protect capabilities. Modeling and simulations are used extensively to support the combat development process. The Advanced Programs Division acts as the IO combat developer, in close coordination with TRADOC. The Division explores lethal, non-lethal, destructive, and nondestructive means to meet information dominance requirements in peacetime, conflict, war, and military operations other than war (MOOTW). The Advanced Programs Division is the focal point for technology transfer opportunities.

Support Division

The Support Division consolidates LIWA intelligence and support activities. The Division manages the overall support functions including security, intelligence, information management, and resource management. Members of the Support Division may augment other LIWA teams during deployments, as required.

Interrelationships

As noted in Figure 3-2, LIWA interfaces with numerous agencies and organizations within the intelligence community, the Army Staff, supported commands, TRADOC, AMC, other services, and National agencies to coordinate IO. In some cases the LIWA provides resident liaison personnel to assist with daily IO support missions. Conversely, some organizations have liaison personnel assigned to the LIWA to coordinated other service and organization strategic and operational level missions. These relationships, Figure 3-4, enables LIWA to rapidly coordinated the sensitive and critical components of strategic IO planning.

---

[2] **Army Rapid Reprogramming Analysis Team Program Office (ARAT PO): Established in 1994 with a charter through 1999, the ARAT PO acts as the technical intermediary between the CECOM Systems Engineering Center and ARAT-TA on matters related to rapid reprogramming of Army Target Sensing Systems (ATSS). ARAT PO developed the Memory Loader Verified (MLV) to reprogram the memory of ATSS when the threat changes, or when the Army deploys to an operational area with a threat array unlike the one the deploying unit' TSS were programmed to handle.**

LIWA Interrelationships	
LIWA's relationship with other elements varies as its missions change. This table illustrates the wide variety of organizations LIWA interfaces with or receives direction from on a continuing basis.	
Organization	**Relationship**
ARSTAF	DCSOPS IO Policy, Operational tasking authority DCSINT Intel policy, NFIP billet management DISC4 C2 systems protect policy, tasking
Intelligence Community	NSA Requests for IO products and support DIA Database support, intel products INSCOM LIWA's parent command NGIC Requests for IO products and support
TRADOC	Headquarters Continuous IO coordination CAC Proponent for IO USAICS Intel doctrine, training, combat developments
AMC	PEO-IEW&S Systems development topics PEO-C3S Red Team support, vulnerability analysis
Other IO Organizations USAF USN USMC NSA JCS	 AFIWC Close coordination FIWC Close coordination NIWC Close coordination IO POC Coordination on a case-by-case basis IO Center Daily interface and exchanges JC2WC Frequent exchanges, exercise coordination

Figure 3-4, LIWA Interrelationships

Tailored support is provided on a case-by-case basis depending on the needs of the supported command. Type of support provided as shown in Figure 3-5, and composition of the various teams is determined through coordination between the supported command and LIWA; DA DCSOPS-OD is the ARSTAF approving authority.

LIWA Support to Army Commands	
Army Commands	**Type Support**
Field Commands Joint Land Component Cmd Corps Divisions Other Organizations	 FST, Red Team, ACERT, ARAT-TA FST, Red Team, ACERT, ARAT-TA FST, Red Team, ACERT, ARAT-TA Tailored support as required
Institutional Commands TRADOC Wargames TRADOC AWEs CAC BCTP CAC Warfighters Army Service Component	 Tailored support as required Red Team, FST FST FST Tailored support as required

Figure 3-5, LIWA Support to Army Commands

Figure 3-6, The Information Operations Foundation, graphically illustrates LIWA's role supporting both the operational and institutional components of the U.S. Army. As an INSCOM activity, working closely with the ARSTAF, LIWA supports or exchanges information within the Army and DoD. On a mission basis, LIWA interfaces with non-DoD agencies and bureaus.

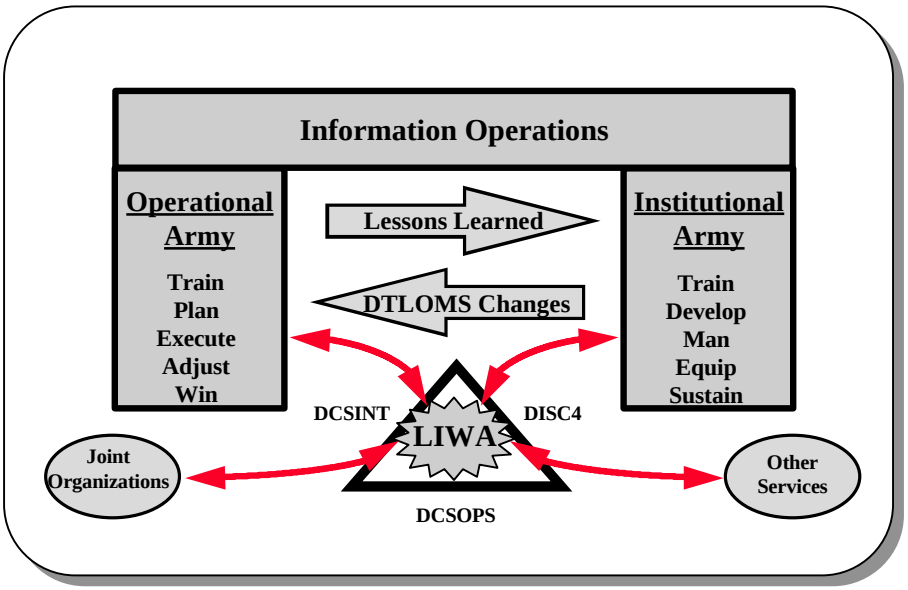

Figure 3-6, The Information Operations Foundation

Type Operations and Core Competencies

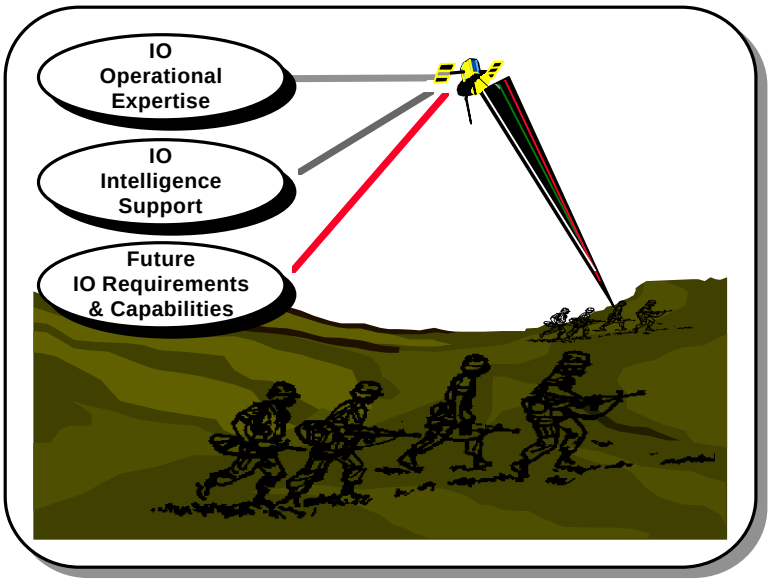

Figure 3-7, Core Competencies

As depicted in Figure 3-7, LIWA functions combine into three interrelated core competencies: IO Operations, IO Intelligence Support, and Future IO Requirements. Combined, these core competencies significantly enhance the Total Army's ability to achieve and sustain Information Dominance across the full spectrum of military operations.

IO Operational Expertise: LIWA's Operations Division contains a mix of military and DA civilian personnel with a variety of skills including combat arms, special operations, aviation, communications and computer specialists, and intelligence analysts. Personnel with tactical and operational-level training and experience and are capable of operating in joint and combined operational environments. Contractor personnel with additional specialties augment the Operations Division as required. The IO operational expertise (C2-Attack, C2-Protect, and C2-Exploit) represented by this array of skills and experience is task organized on a mission-by-mission basis into teams, and deployed to support Army commands.

IO Intelligence Support: LIWA's structure contains a small intelligence organization designed to be the focal point for IO intelligence support. The value of this organization resides in its ability to respond rapidly to field-generated, IO-unique intelligence requirements, and to forward and track requests for IO intelligence support. A mix of intelligence specialties, supported by automation and connectivity to DIA, NSA, joint intelligence centers and IW cells of the other services, allows LIWA to request and receive IO specific data from multiple sources. In addition, LIWA provides liaison personnel to selected intelligence organizations, increasing their awareness of Army IO needs and facilitating the exchange of IO-related intelligence. LIWA intelligence analysts provide deployed teams with sharply focused IO area studies, IO targeting products, and quick-response one-of-a-kind reports designed to meet specific needs from the field.

Future IO Requirements and Capabilities: LIWA conducts and participates in studies, wargames and exercises designed to identify future IO requirements and capabilities. Models and simulations are developed to support analysis and decision making. Working closely with government, industry, and academia, LIWA looks for opportunities to apply advanced technology against IO requirements using commercial, off-the-shelf hardware and software. The dynamic nature of C2-related technology, and RDA funding constraints places a premium on off-the-shelf applications, and low density procurements. Information Operations, directed against opponents employing advanced commercial C2 systems, may require state-of-the-art systems to effectively attack, exploit, an opponent's C2 systems, or to protect friendly systems.

The following matrix portrays the type of operations LIWA supports and the LIWA core compabilities associated with each.

Type Operation	LIWA Core Capabilities
Contingency Operations	Field Support Teams can be tailored to provide the type of support commands require. Capabilities provided range from one or two people to provide advice, to a robust team able to comprehensively monitor ongoing IO. Combinations of the following competencies may be employed: a. Planning IO operations b. Identifying and selecting IO targets c. Coordinating PSYOP, OPSEC, Deception, EW and Destruction d. Integrating CA, PA, and other US and coalition elements into an operation. e. Identifying IO communications requirements f. Coordinating with external commands, agencies and activities supporting IO. g. Maintaining a running status of ongoing IO, briefing as needed h. Integrating intelligence into IO

	i. Establishing and maintaining FST communications.
Type Operation	**LIWA Core Capabilities**
Information Operations Planning **CONPLAN Development** **CONPLAN Review** **BCTP Planning** **Warfighter Exercises** **CONPLAN Exercises** **Wargames** **AWEs**	**LIWA FSTs planning support to commands includes:** **a. IO mission analysis** **b. Course of action development and wargaming** **c. Development of decision briefings** **d. Development of the IO Annex, to including intelligence taskings and requests.** **e. Coordinate, synchronize, and deconflict all facets of IO internally and with external commands.** **f. Establish linkages to Army, other services, DOD agencies and the joint or combined command IO elements.** **Support of wargame and exercise planning carries the additional requirement to help construct the scenario and events' lists, and to help insert IO factors into models and simulations.**
C2 Vulnerability Assessments	**The Red Team, frequently with support from ACERT and Field Support Team elements, is charged with looking at friendly forces through the eyes of an opponent. To achieve this goal, the Red Team** **a. Identifies the vulnerability assessment needs of the supported command.** **b. Determines manpower, system, communications, and mission support requirements.** **c. Coordinates schedule** **d. Develops, coordinates, and implements a collection and analysis plan.** **e. Compiles vulnerability assessment report** **f. Outbrief the supported command** **When C2 vulnerabilities are identified the Red Team notifies the supported command and helps the command make adjustments to eliminate, reduce, or control the vulnerability. Ideally, adjustments can be assessed for effectiveness while the Red Team's collection and analysis assets are still supporting the mission.**
Computer Emergency Response	**The Army Computer Emergency Response Team (ACERT) is available to Army commands experiencing attempted computer penetrations, data contamination, disruptions, etc. The ACERT provides:** **a. Diagnostic support** **b. Help to determine if hackers were involved** **c. Assistance getting equipment back into operation** **d. Support to apply safeguards and other system management tools** **e. Alerts to warn of possible attacks** **f. Coordination with investigating agencies, if needed** **g. Reports to the ARSTAF as required**
Sensor Reprogramming	**The Army Reprogramming Analysis Team-Threat Assessment (ARAT-TA) is collocated with the Air Force's reprogramming element at Hurlbert AFB, Florida. The ARAT-TA:** **a. Assesses the technical threat environment of an operational or contingency area.** **b. Determines when parametric data changes are required sensing systems of weapon systems.** **c. Notifies the appropriate program manager of changes needed.** **d. Sends appropriate parametric data to affected units.** **e. Coordinates and shares data with other services' reprogramming elements.**
IO Modeling and Combat Developments	**Advanced programs support has applications across LIWA and to Army combat and materiel developers. Advanced programs includes:** **a. IO model and simulation development** **b. Automated decision support tool development** **c. Combat development of IO-type systems** **d. The application of advanced technology to meet IO requirements.**
Mission Support	**LIWA's teams require a wide range of backup support to operate effectively. Support includes:** **a. Maintain communications with deployed teams.** **b. Provide tailored intelligence studies and reports.** **c. Assist in the application of advanced technology.** **d. Maintain liaison with other services, agencies and commands in Teams' behalf.** **e. Provide or dispatch back up support.**

1

Mobilization and Reserve Component Integration

The LIWA is heavily dependent upon both Individual Mobilization Augmentees (IMAs) and Drilling Individual Mobilization Augmentees (DIMAs) to provide valuable IO support during crisis periods.

IMAs and DIMAs will serve in the LIWA Support Center providing intelligence and communications support to deployed LIWA Field Support Teams (FST). Support includes C2W Target Folders, Information IPB studies, and specialized C2W area studies. Reservists assigned to LIWA Field Support Teams contribute to OPLAN IO planning and targeting for Army commands and perform specialized C2W targeting and intelligence functions. Reservists will also augment the Army Computer Emergency Response Team contributing to the protection of Army computer systems and networks.

Command and Control

The Commander, Headquarters Intelligence and Security Command (INSCOM-IAOPS) provides command, personnel, resources, security, UCMJ authority, administration, and logistics support for the LIWA. HQDA (DAMO-ODI), Director of Operations, Readiness and Mobilization exercises operational tasking authority of the LIWA including IW, IO, and C2W operational support policy and program planning guidance.

Tasking Channels

As shown in Figure 3-7, Army organizations should address messages and correspondence requesting LIWA assistance to one of the following, with copy furnished to Director LIWA.

DAMO-ODI Mail and Message Traffic	
Type Traffic	**Address**
Mail	HQDA ATTN: DAMO-ODI 400 Army Pentagon, Washington, DC 20310-0400
GENSER	HQDAWASHDC//DAMO-ODI//

Figure 3-7, DAMO-ODI Mail and Message Traffic

Informal contact and coordination between the requesting command and LIWA are encouraged and should be exercised extensively as soon as a request for support is contemplated. As shown in Figure 3-8, contact with the Director LIWA or his staff can be established using any of the following means:

LIWA Telephone Numbers		
Means	**Commercial**	**DSN**
Telephone Director LIWA LIWA Support Center Action Desk ACERT (24 hours per day) ARAT-TA INSCOM Operations Center (24 hours per day operation)	 (703) 706-2266 (703) 706-1165 1-888-203-6322 (904) 882-8899 (703) 706-2000	 235 235 n/a 872 235
Unsecure Facsimile	(703) 806-1003	656
Secure Facsimile	(703) 806-1004	656

Figure 3-8, LIWA Telephone Numbers

LIWA Mail and Message Addresses	
Type Traffic	**Address**
Mail	Commander, USAINSCOM, ATTN: LIWA (Name of Person), 8825 Beulah Street. FT Belvoir, VA 22060-5246
GENSER	RUDHIWC/DIRLIWA FT BELVOIR VA//
MILNET	liwa@vulcan.belvior.army.mil

Figure 3-8, LIWA Mail and Message Addresses

Validation and Approval Authorities

All request for LIWA support will be validated and approved by HQ Department of Army (DAMO-ODI). Requesting organizations will receive confirmation of all requested support through official communication channels.

Upon receipt of the request, DAMO-ODI coordinates the action within the ARSTAF, JCS, and other services and agencies if required, and with the Director LIWA and the G3 INSCOM. DAMO-ODI either tasks INSCOM (LIWA) to provide the requested support, or adjusts support requirements in coordination with the requesting command. Organizations requesting LIWA support are cautioned not to irreversibly plan for LIWA assistance until confirmation is received. LIWA priorities for support, as directed by the Army Vice Chief of Staff, are:

1. Contingency Operations
2. Army XXI Initiatives
3. Combat Training Center Exercises (BCTP, JRTC, NTC, AAN etc.)
4. Service School Support
5. Routine Operational Support