Change No. 3

FM 7-15, C3
Headquarters
Department of the Army
Washington, DC, 29 July 2010

The Army Universal Task List

1. Change 3 to FM 7-15, 27 February 2009, replaces chapter 2 to align intelligence collective tasks and current intelligence doctrine as a result of the recently published FM 2-0.
2. A bar (⎪) marks new material.
3. FM 7-15, 27 February 2009, is changed as follows:

Remove Old Pages	**Insert New Pages**
pages i through iv	pages i through iv
pages 2-1 through 2-54	pages 2-1 through 2-54

4. File this transmittal sheet in front of the publication for reference purposes.

DISTRIBUTION RESTRICTION: Approved for public release; distribution is unlimited.

FM 7-15, C3
July 2010

By order of the Secretary of the Army:

GEORGE W. CASEY, JR.
General, United States Army
Chief of Staff

Official:

JOYCE E. MORROW
Administrative Assistant to the
Secretary of the Army
1020103

DISTRIBUTION:
Active Army, Army National Guard, and U.S. Army Reserve: Not to be distributed; electronic media only.

PIN: 081007-003

Field Manual
No. 7-15

Headquarters
Department of the Army
Washington, DC, 27 February 2009

The Army Universal Task List

Contents

Page

PREFACE ..... **ix**

INTRODUCTION ..... **xii**

Chapter 1 **ART 1.0: THE MOVEMENT AND MANEUVER WARFIGHTING FUNCTION** .. **1-1**

Section I – ART 1.1: Perform Tactical Actions Associated with Force Projection and Deployment **1-2**

ART 1.1.1 Conduct Mobilization of Tactical Units 1-2
ART 1.1.2 Conduct Tactical Deployment/Redeployment Activities 1-4
ART 1.1.3 Conduct Demobilization of Tactical Units 1-7
ART 1.1.4 Conduct Rear Detachment Activities 1-7

Section II – ART 1.2: Conduct Tactical Maneuver **1-8**

ART 1.2.1 Conduct One of the Five Forms of Maneuver 1-9
ART 1.2.2 Employ Combat Formations 1-11
ART 1.2.3 Employ Combat Patrols 1-17
ART 1.2.4 Conduct Counterambush Actions 1-17
ART 1.2.5 Exploit Terrain to Expedite Tactical Movements 1-18
ART 1.2.6 Cross a Danger Area 1-18
ART 1.2.7 Link Up with Other Tactical Forces 1-18
ART 1.2.8 Conduct Passage of Lines 1-19
ART 1.2.9 Conduct a Relief in Place 1-20
ART 1.2.10 Navigate from One Point to Another 1-21
ART 1.2.11 Conduct a Survivability Move 1-21
ART 1.2.12 Conduct Sniper Active Countermeasures 1-22
ART 1.2.13 Conduct Sniper Passive Countermeasures 1-22

Section III – ART 1.3: Conduct Tactical Troop Movements **1-23**

ART 1.3.1 Prepare Forces for Movement 1-23
ART 1.3.2 Conduct Tactical Road March 1-25
ART 1.3.3 Conduct Tactical Convoy 1-25
ART 1.3.4 Conduct an Approach March 1-26

Distribution Restriction: This manual is approved for public release; distribution is unlimited.

***This publication supersedes FM 7-15, 31 August 2003.**

Section IV – ART 1.4: Conduct Direct Fires 1-27
ART 1.4.1 Conduct Lethal Direct Fire Against a Surface Target 1-27
ART 1.4.2 Conduct Nonlethal Direct Fire Against a Surface Target 1-28
Section V – ART 1.5: Occupy an Area 1-29
ART 1.5.1 Occupy an Assembly Area 1-29
ART 1.5.2 Occupy an Attack and Assault Position 1-29
ART 1.5.3 Occupy and Establish a Battle or Defensive Position 1-30
ART 1.5.4 Conduct Drop Zone Operations 1-30
ART 1.5.5 Conduct Landing Zone Operations 1-31
Section VI – ART 1.6: Conduct Mobility Operations 1-32
ART 1.6.1 Overcome Barriers, Obstacles, and Mines 1-33
ART 1.6.2 Enhance Movement and Maneuver 1-38
ART 1.6.3 Negotiate a Tactical Area of Operations 1-41
ART 1.6.4 Provide Diver Support 1-41
ART 1.6.5 Conduct Nontactical Movements 1-42
Section VII – ART 1.7: Conduct Countermobility Operations 1-43
ART 1.7.1 Site Obstacles 1-44
ART 1.7.2 Construct, Emplace, or Detonate Obstacles 1-45
ART 1.7.3 Mark, Report, and Record Obstacles 1-45
ART 1.7.4 Maintain Obstacle Integration 1-46
Section VIII – ART 1.8: Employ Obscurants 1-46

Chapter 2 ART 2.0: THE INTELLIGENCE WARFIGHTING FUNCTION 2-1
Section I – ART 2.1: Intelligence Support to Force Generation 2-2
ART 2.1.1 Provide Intelligence Readiness 2-2
ART 2.1.2 Establish Intelligence Architecture 2-4
ART 2.1.3 Provide Intelligence Overwatch 2-8
ART 2.1.4 Generate Intelligence Knowledge 2-8
ART 2.1.5 Tailor the Intelligence Force 2-13
Section II – ART 2.2: Support to Situational Understanding 2-15
ART 2.2.1 Perform Intelligence Preparation of the Battlefield 2-16
ART 2.2.2 Perform Situation Development 2-20
ART 2.2.3 Provide Intelligence Support to Protection 2-20
ART 2.2.4 Provide Tactical Intelligence Overwatch 2-21
ART 2.2.5 Conduct Police Intelligence Operations 2-21
ART 2.2.6 Provide Intelligence Support to Civil Affairs Activities 2-26
Section III – ART 2.3: Perform Intelligence, Surveillance, and Reconnaissance 2-27
ART 2.3.1 Perform Intelligence, Surveillance, and Reconnaissance Synchronization 2-28
ART 2.3.2 Perform Intelligence, Surveillance, and Reconnaissance Integration 2-30
ART 2.3.3 Conduct Reconnaissance 2-33
ART 2.3.4 Conduct Surveillance 2-38
ART 2.3.5 Conduct Intelligence Related Missions and Operations 2-38
Section IV – ART 2.4: Support to Targeting and Information Superiority . 2-46
ART 2.4.1 Provide Intelligence Support to Targeting 2-47

ART 2.4.2 Provide Intelligence Support to Army Information Tasks 2-48
ART 2.4.3 Provide Intelligence Support to Combat Assessment 2-53

Chapter 3 ART 3.0: THE FIRES WARFIGHTING FUNCTION 3-1
Section I – ART 3.1: Decide Surface Targets 3-1
Section II – ART 3.2: Detect and Locate Surface Targets 3-2
Section III – ART 3.3: Provide Fire Support 3-2
ART 3.3.1 Conduct Fires 3-3
ART 3.3.2 Provide Illumination 3-7
ART 3.3.3 Conduct Survey Operations in Support of Fires Systems 3-8
ART 3.3.4 Perform Meteorological Operations in Support of Fires Systems 3-8
ART 3.3.5 Conduct Suppression of Enemy Air Defenses 3-9
Section IV – ART 3.4: Integrate Command and Control Warfare 3-10
ART 3.4.1 Conduct Electronic Attack 3-10
ART 3.4.2 Nominate Computer Network Attack Targets 3-11
ART 3.4.3 Nominate Electronic Attack Targets 3-11

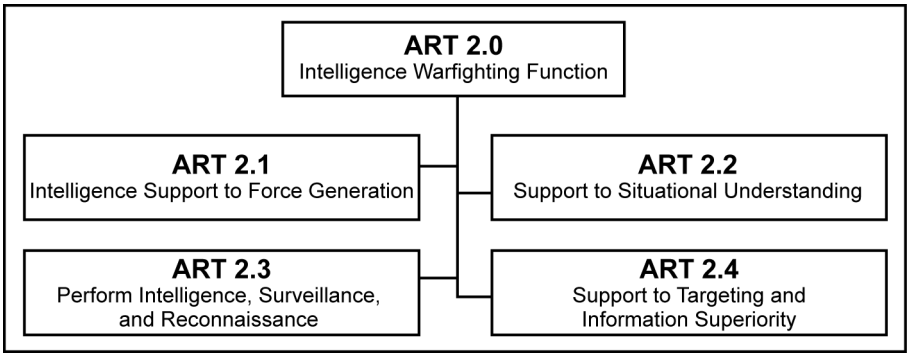
Chapter 4 ART 4.0: THE SUSTAINMENT WARFIGHTING FUNCTION 4-1
Section I – ART 4.1: Provide Logistics Support 4-2
ART 4.1.1 Provide Maintenance Support 4-3
ART 4.1.2 Provide Transportation Support 4-7
ART 4.1.3 Provide Supplies 4-15
ART 4.1.4 Provide Field Services 4-32
ART 4.1.5 Provide Contracting Support 4-38
ART 4.1.6 Provide Distribution 4-39
ART 4.1.7 Provide General Engineer Support 4-44
Section II – ART 4.2: Provide Personnel Services Support 4-64
ART 4.2.1 Provide Human Resources Support 4-65
ART 4.2.2 Provide Financial Management Support 4-73
ART 4.2.3 Provide Legal Support 4-77
ART 4.2.4 Plan Religious Support Operations 4-82
ART 4.2.5 Provide Band Support 4-85
Section III – ART 4.3: Provide Health Service Support 4-86
ART 4.3.1 Provide Combat Casualty Care 4-86
ART 4.3.2 Provide Medical Evacuation (Air and Ground) 4-90
ART 4.3.3 Provide Medical Regulating Support 4-91
ART 4.3.4 Provide Medical Logistics 4-91
Section IV – ART 4.4: Conduct Internment and Resettlement Operations 4-94
ART 4.4.1 Perform Internment Operations 4-94
ART 4.4.2 Conduct Resettlement Operations 4-97
ART 4.4.3 Conduct Resettlement Operations ..... Rescinded

Chapter 5 ART 5.0: CONDUCT COMMAND AND CONTROL 5-1
Section I – ART 5.1: Execute the Operations Process 5-2
ART 5.1.1 Plan Operations 5-2
ART 5.1.2 Prepare for Tactical Operations 5-8
ART 5.1.3 Execute Tactical Operations 5-11

ART 5.1.4 Assess Tactical Situations and Operations 5-17
Section II – ART 5.2: Conduct Command Post Operations 5-21
ART 5.2.1 Conduct Command Post Operations to Support Tactical Operations 5-22
ART 5.2.2 Displace the Command Post 5-23
ART 5.2.3 Execute Sleep Plans 5-24
ART 5.2.4 Manage Stress 5-25
ART 5.2.5 Maintain Continuity of Command and Control 5-25
Section III – ART 5.3: Integrate Information Superiority Contributors 5-26
ART 5.3.1 Integrate Information Engagement Capabilities 5-26
ART 5.3.2 Conduct Military Deception 5-29
ART 5.3.3 Facilitate Situational Understanding Through Knowledge Management 5-30
ART 5.3.4 Manage Information and Data 5-30
ART 5.3.5 Establish the Information Network and System 5-30
ART 5.3.6 Conduct Electromagnetic Spectrum Management Operations 5-35
Section IV – ART 5.4: Conduct Civil-Military Operations 5-37
ART 5.4.1 Provide Interface or Liaison Among Military and Civilian Organizations 5-38
ART 5.4.2 Locate and Identify Population Centers 5-39
ART 5.4.3 Identify Local Resources, Facilities, and Support 5-39
ART 5.4.4 Advise Commanders of Obligations to Civilian Population 5-40
ART 5.4.5 Conduct Negotiations With and Between Other Government Agencies and Nongovernmental Organizations 5-41
ART 5.4.6 Conduct Civil Affairs Operations 5-42
Section V – ART 5.5: Execute Command Programs 5-59
ART 5.5.1 Support the Commander's Leadership Responsibilities for Morale, Welfare, and Discipline 5-59
ART 5.5.2 Preserve Historical Documentation and Artifacts 5-67
ART 5.5.3 Conduct Official Ceremonial, Musical, Public, and Special Events 5-72
ART 5.5.4 Develop a Command Environmental Program 5-72
Section VI – ART 5.6: Integrate Space Operations 5-73
ART 5.6.1 Provide Space Force Enhancement 5-74
ART 5.6.2 Provide Space Control 5-75
ART 5.6.3 Provide Army Space Support 5-76
ART 5.6.4 Provide Space Situational Awareness 5-76.1
ART 5.6.5 Coordinate Army Space Capabilities 5-76.2
Section VII – ART 5.7: Conduct Public Affairs Operations 5-77
ART 5.7.1 Plan Public Affairs Operations 5-77
ART 5.7.2 Execute Information Strategies 5-77
ART 5.7.3 Facilitate Media Operations 5-78
ART 5.7.4 Maintain Community Relations 5-78
ART 5.7.5 Conduct Internal Information Program 5-79
ART 5.7.6 Implement Higher Headquarters Public Affairs Themes 5-79
Section VIII – ART 5.8: Establish and Maintain Discipline 5-79
ART 5.8.1 Conduct Law and Order Operations 5-80
ART 5.8.2 Intern U.S. Military Prisoners 5-85

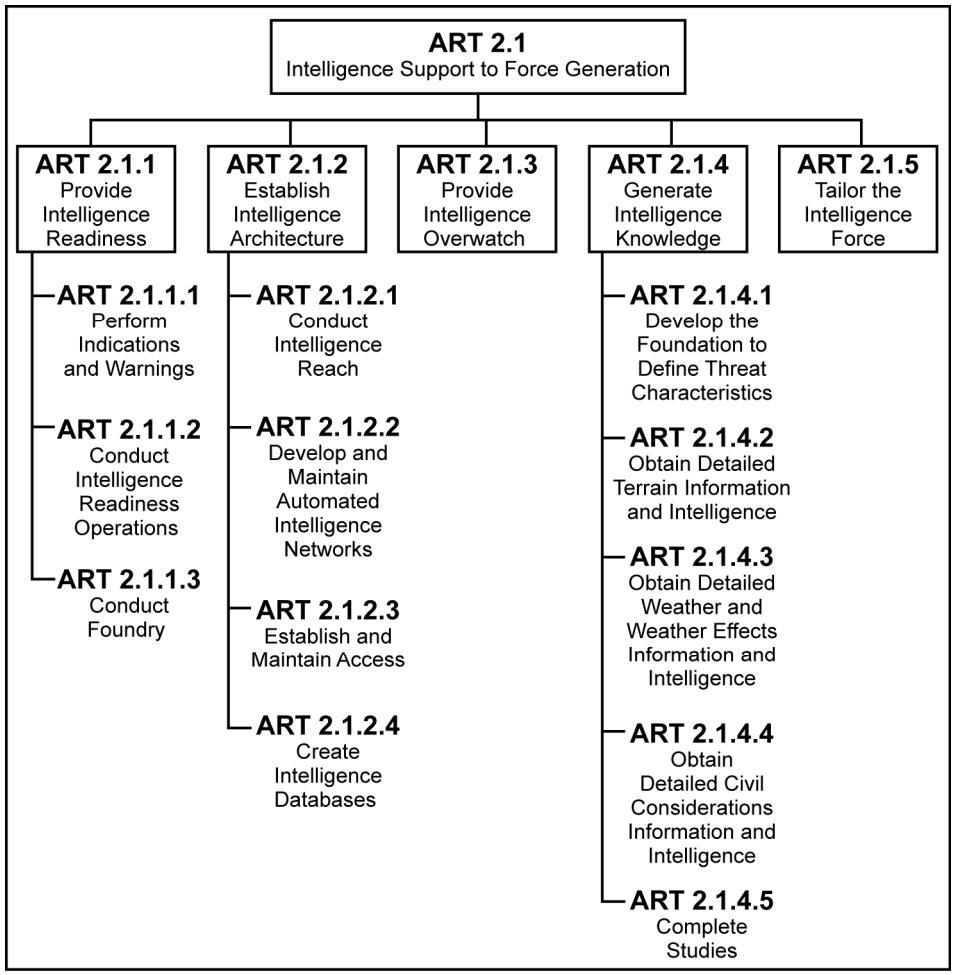
Chapter 2

ART 2.0: The Intelligence Warfighting Function



The *intelligence warfighting function* is the related tasks and systems that facilitate understanding of the operational environment, enemy, terrain, and civil considerations. It includes tasks associated with intelligence, surveillance, and reconnaissance operations, and is driven by the commander. Intelligence is more than just collection. As a continuous process, it involves analyzing information from all sources (human, imagery, measurement and signature, signal) and conducting operations to develop the situation. (FM 3-0) (USACAC)

SECTION I – ART 2.1: INTELLIGENCE SUPPORT TO FORCE GENERATION



2-1. Intelligence support to force generation is the task of generating intelligence knowledge concerning an area of interest, facilitating future intelligence operations, and tailoring the force. It includes establishing intelligence communication and knowledge management architectures. These architectures enable collaboration among strategic, operational, and tactical intelligence organizations in the following areas—intelligence reach; collaborative analysis; data storage; processing and analysis; and intelligence production support to force generation consists of five tasks. (FM 2-0) (USAICoE)

ART 2.1.1 PROVIDE INTELLIGENCE READINESS

2-2. Intelligence readiness operations develop baseline knowledge of multiple potential threats and operational environments. These operations support ongoing operations, contingency planning, and operational preparation. These operations and related intelligence training activities enable the intelligence warfighting function to support the commander's intelligence requirements effectively. (FM 2-0) (USAICoE)

No.	Scale	Measure
01	Yes/No	Unit provided indications and warning reports.
02	Yes/No	Unit provided intelligence readiness.
03	Yes/No	Unit conducted foundry training.
04	Percent	Of intelligence relating to indications and warning prior to incident occurring.
05	Percent	Of relevant data, information, intelligence, and products received on the operational environment.
06	Percent	Of relevant training received for the conduct of operations.

ART 2.1.1.1 PERFORM INDICATIONS AND WARNING

2-3. This task provides the commander with advance warning of threat actions or intentions. The intelligence officer develops indications and warnings to rapidly alert the commander of events or activities that would change the basic nature of the operation. It enables the commander to quickly reorient the force to unexpected contingencies and shape the operational environment. (FM 2-0) (USAICoE)

No.	Scale	Measure
01	Yes/No	Unit issued indications and warnings in sufficient time to prevent the enemy or threat from surprising the targeted friendly unit or installation.
02	Yes/No	Unit disseminated indications and warnings after development and compared to other information and intelligence to ensure accuracy.
03	Yes/No	Intelligence officer monitored event template and matrix to determine if the enemy or threat was performing a predicted course of action (COA).
04	Yes/No	Unit identified enemy and potential threats in the operational environment.
05	Yes/No	Unit updated enemy and threat identification, tactics, techniques, and procedures.
06	Time	Between receipt of significant information and intelligence and updates of indications and warnings conditions.
07	Time	To conduct predictive analysis in support of COA development.
08	Time	To predict significant changes in enemy or threat activities.
09	Time	Required to disseminate indications and warnings to appropriate echelons, agencies, and organizations.
10	Time	To submit intelligence portion of commander's situation report.
11	Percent	Of indications and warnings of threat actions reported that will impact friendly forces operations.
12	Percent	Of commander's threat conditions and attack warnings issued and disseminated.
13	Percent	Of threat indicators maintained and evaluated.

ART 2.1.1.2 CONDUCT INTELLIGENCE READINESS OPERATIONS

2-4. Intelligence readiness operations support contingency planning and preparation by developing baseline knowledge of multiple potential threats and operational environments. This information and training enables a collaborative effort and environment to provide the best possible initial threat understanding. (FM 2-0) (USAICoE)

No.	Scale	Measure
01	Yes/No	Unit provided information on the civil considerations using the factors of areas, structures, capabilities, organizations, people and events affecting the force.
02	Percent	Of intelligence relating to the enemy force.
03	Percent	Of intelligence relating to potential terrorist acts against U.S. forces.
04	Percent	Of intelligence relating to potential insurgent, guerrilla, or criminal groups.
05	Percent	Of intelligence relating to using chemical, biological, radiological, nuclear, and high-yield explosives (CBRNE) weapons.

No.	Scale	Measure
06	Percent	Of information and intelligence that facilitates a cultural understanding of the operational environment.
07	Percent	Of intelligence requirements to support the other warfighting functions or Army programs.

ART 2.1.1.3 CONDUCT FOUNDRY

2-5. Foundry is a training program designed to sustain critical intelligence capabilities and perishable intelligence skills, and provide regional focus, technical training and functional expertise to the tactical military intelligence (MI) force through home-station training platforms, mobile training teams, and live environment training opportunities. Foundry creates a single hub for advanced skills training across the Active Army, Army National Guard, and the Army Reserve MI force. It also provides training to leaders who supervise MI missions and Soldiers who perform MI activities. (FM 2-0) (USAICoE)

No.	Scale	Measure
01	Yes/No	Unit identified specific intelligence skills by each military occupational specialty needed to deploy to a specific theater.
02	Yes/No	Unit identified intelligence training requirements and skills needed for MI sustainment and the intelligence overwatch program.
03	Yes/No	Unit identified intelligence training resources available to conduct foundry training in order to meet theater specific mission and deployment standards.
04	Yes/No	Unit prepared foundry prioritized quarterly training requests for funding.
05	Yes/No	MI soldiers and units actively participated in foundry training opportunities to include live environment training.
06	Yes/No	Unit established unit and functional partnerships in support of MI training and readiness effort.
07	Yes/No	Unit used Project Foundry to develop MI adjunct faculty (subject matter expert) in support of unit and home station training efforts.
08	Yes/No	Unit conducted MI periodic training councils to share training resources and assets.
09	Yes/No	Units used Project Foundry to conduct unit collective training and for unit exercises.
10	Yes/No	Units reported tactics, techniques, and procedures (TTP) and lessons learned for integration into training programs, doctrine, and the Project Foundry.
11	Yes/No	Unit conducted an annual assessment of Project Foundry and MI training successes and needs.
12	Percent	Of unfunded quarterly foundry training requests.
13	Number	Of skills identified for deployment used in theater.
14	Number	Of skills not initially identified but were needed in theater.
15	Number	Of available MI soldiers requiring training who participate annually in foundry training.
16	Number	Of available MI units requiring training who participate annually in foundry training.
17	Number	Of units that utilize foundry for collective training.
18	Number	Of units that utilize foundry for unit exercises.
19	Number	Of units that report TTP and lessons learned for integration into training programs, doctrine, and the Project Foundry.
20	Number	Of items identified in the annual assessment needed to improve Project Foundry and MI training.

ART 2.1.2 ESTABLISH INTELLIGENCE ARCHITECTURE

2-6. Establishing an intelligence architecture includes complex and technical issues that include hardware, software, communications, communications security materials, network classification, technicians, database access, liaison officers, training, and funding. Well-defined and well-designed intelligence architecture can offset or mitigate structural, organizational, or personnel limitations. This architecture

provides the best possible understanding of the threat, terrain, and weather, and civil considerations understanding. (FM 2-0) (USAICoE)

No.	Scale	Measure
01	Yes/No	Unit identified national agencies with relevant information, databases, and systems to form a collaborative environment.
02	Yes/No	Unit identified Department of Defense organizations with relevant information, databases, and systems to form a collaborative environment.
03	Yes/No	Unit identified multinational organizations and elements with relevant data, information, databases, and systems to form a collaborative environment.
04	Yes/No	Unit identified Army organizations with relevant information, databases, and systems to form a collaborative environment.
05	Yes/No	Unit achieved enemy and threat understanding through the intelligence architecture.
06	Percent	Of analysis, training, and intelligence production achieved through collaborative intelligence architecture.
07	Percent	Of structural, organizational, or personnel limitations offset or mitigated.

ART 2.1.2.1 CONDUCT INTELLIGENCE REACH

2-7. Intelligence reach is a process by which intelligence organizations proactively and rapidly access information from, receive support from, and conduct direct collaboration and information sharing with other units and agencies, both within and outside the area of operations, unconstrained by geographic proximity, echelon, or command. Intelligence obtained through intelligence reach helps the staff plan and prepare for operations and answer commander's critical information requirements without the need for the information to pass through a formal hierarchy. (FM 2-0) (USAICoE)

No.	Scale	Measure
01	Yes/No	Unit established unit procedures or processes by which to conduct intelligence reach.
02	Yes/No	Soldiers trained, maintained, exercised, and sustained their intelligence reach procedures or processes.
03	Yes/No	Unit received information or intelligence through intelligence reach relevant to operations.
04	Yes/No	Unit used intelligence reach in intelligence, surveillance, and reconnaissance (ISR) planning.
05	Time	Required to update procedures and processes for intelligence reach sustainment.
06	Percent	Of trained personnel on intelligence reach procedures.
07	Percent	Of relevant information obtained.
08	Percent	Of information acquired through organic ISR taskings available through intelligence reach.
09	Percent	Of ISR tasks developed through information obtained by intelligence reach.
10	Percent	Of ISR tasks dynamically retasked due to information obtained by intelligence reach.

ART 2.1.2.2 DEVELOP AND MAINTAIN AUTOMATED INTELLIGENCE NETWORKS

2-8. This task entails providing information systems that connect unique assets, units, echelons, agencies, and multinational partners for intelligence, collaborative analysis and production, dissemination, and intelligence reach. It uses existing automated information systems, such as the distributed common ground system-Army (known as DCGS-A), and, when necessary, creates operationally specific networks. In either case, these networks allow access to unclassified and classified means, and interoperability across the area of operations. This task includes identifying deficiencies in systems or networks, Service procedures, system administration procedures, security procedures, alternate power plan, redundancy capability, system backups, and update procedures. (FM 2-0) (USAICoE)

No.	Scale	Measure
01	Yes/No	Unit established intelligence specific networks (classified and unclassified).
02	Yes/No	The appropriate unique assets, units, echelons, agencies, and multinational partners were included in the network.

No.	Scale	Measure
03	Yes/No	The intelligence network was used for collaborative analysis and production, dissemination, and intelligence reach.
04	Yes/No	The intelligence network was adequate for collaborative analysis and production, dissemination, and intelligence reach.
05	Yes/No	The intelligence network was adequate for interoperability across the area of operations to include subordinate elements collaborative analysis and production, dissemination, and intelligence reach.
06	Yes/No	Policies and procedures were in place for identifying deficiencies in the systems or networks.
07	Yes/No	Policies and procedures were in place for implementing service procedures and an alternate power plan.
08	Yes/No	Policies and procedures were in place for network security.
09	Yes/No	Policies and procedures were in place for system backup and update.
10	Yes/No	Units used policies and procedures for system administration.
11	Yes/No	Adequate redundancy was built into the network.
12	Time	The network was down or unavailable due to service, system administration, or system update.
13	Time	Between the primary system failing and the redundancy capability initialized.
14	Percent	Of network used for collaborative analysis and production, dissemination, and intelligence reach.
15	Percent	Of time the redundancy capability was used in place of the primary system.

ART 2.1.2.3 ESTABLISH AND MAINTAIN ACCESS

2-9. Establish and provide access to classified and unclassified programs, databases, networks, systems, and other Web-based collaborative environments for Army and multinational organizations to facilitate intelligence reporting, production, dissemination, sustainment, and intelligence reach. This task also includes establishing access to classified and unclassified programs, databases, networks, systems, and other Web-based collaborative environments with joint forces and national agencies to facilitate a multilevel collaborative information environment. This task entails establishing, providing, and maintaining access to classified and unclassified programs, databases, networks, systems, and other Web-based collaborative environments for Army forces, joint forces, national agencies, and multinational organizations. Its purpose is to facilitate intelligence reporting, production, dissemination, and sustainment; intelligence reach; and a multilevel collaborative information environment. (FM 2-0) (USAICoE)

No.	Scale	Measure
01	Yes/No	Unit established or provided access to classified and unclassified programs, databases, networks, systems, and other Web-based collaborative environments for Army and multinational organizations.
02	Yes/No	Unit provided access to classified and unclassified programs, databases, networks, systems, and other Web-based collaborative environments with joint and interagency organizations to facilitate a multilevel collaborative environment.
03	Yes/No	Unit established individual user accounts per applicable policies and regulations and any applicable prerequisite training.
04	Yes/No	Unit established local standing operating procedures (SOPs) for individual user accounts.
05	Yes/No	Unit maintained individual user accounts per the SOPs, policies, regulations, and any applicable recertification or revalidation training.
06	Yes/No	Unit established system accounts per policies, regulations, and any prerequisite training.
07	Yes/No	Unit established local SOPs for system accreditation.
08	Yes/No	Unit established joint, interagency, and multinational accounts per policies, regulations, and any prerequisite training.
09	Yes/No	Unit established local SOPs for joint, interagency, and multinational accounts establishment and maintenance.

No.	Scale	Measure
10	Yes/No	Unit maintained joint, interagency, and multinational accounts per policies, regulations, and any prerequisite training.
11	Yes/No	Unit designated a security officer to ensure local SOPs meet appropriate standards for Army, joint, interagency, and multinational policies and regulations.
12	Yes/No	Unit designated a security officer to establish an oversight or inspection program to enforce Army, joint, interagency, and multinational policies and regulations.
13	Yes/No	Unit designated a security officer to serve as the liaison for higher headquarters, joint, and interagency oversight and inspection teams.

ART 2.1.2.4 CREATE INTELLIGENCE DATABASES

2-10. This task entails creating and maintaining unclassified and classified databases. Its purpose is to establish interoperable and collaborative environments for Army forces, joint forces, national agencies, and multinational organizations. This task facilitates intelligence analysis, reporting, production, dissemination, sustainment, and intelligence reach. It also includes the requirements for formatting and standardization, indexing and correlation, normalization, storage, security protocols, and associated applications. The following must be addressed in database development, management, and maintenance: data sources; information redundancy; import and export standards; data management and standards; update and backup procedures; and data mining, query, and search protocols. (FM 2-0) (USAICoE)

No.	Scale	Measure
01	Yes/No	Unit established and maintained classified and unclassified databases at the appropriate echelons and organizations.
02	Yes/No	Unit established prerequisite training for users on database use; data mining, searches, and queries; and update and backup procedures.
03	Yes/No	Unit established local standing operating procedures (SOPs) for database use; data mining, searches, and queries; and update and backup procedures.
04	Yes/No	The intelligence database was used for collaborative analysis and production, dissemination, and intelligence reach.
05	Yes/No	The intelligence database was adequate for collaborative analysis and production, dissemination, and intelligence reach.
06	Yes/No	The intelligence database was adequate for interoperability across the area of operations to include subordinate elements' collaborative analysis and production, dissemination, and intelligence reach.
07	Yes/No	Policies and procedures were in place for reporting issues with database security and database deficiencies or corruption.
08	Yes/No	Adequate redundancy was built into the database.
09	Yes/No	Policies and procedures were provided for database administration.
10	Yes/No	Unit designated a primary and alternate database manager to ensure local SOPs meet appropriate standards for Army, joint, interagency, and multinational policies and regulations.
11	Yes/No	Unit established training program for the primary and alternate database managers.
12	Yes/No	Policies and procedures were in place for implementing Service procedures and a data redundancy plan.
13	Yes/No	Policies and procedures were in place for database security.
14	Yes/No	Policies and procedures were in place for a database backup and update.
15	Time	That database was down or unavailable due to service, administration, or update.
16	Time	Between the primary database failing and the redundancy capability was initialized.
17	Time	That primary or alternate database manager spent on correcting or resolving deficiencies or corruptions with the primary or redundant database.
18	Percent	Of database used for collaborative analysis and production, dissemination, and intelligence reach.
19	Percent	Of time the redundancy capability was used in place of the primary database.

ART 2.1.3 PROVIDE INTELLIGENCE OVERWATCH

2-11. Intelligence overwatch is creating standing, fixed analytical intelligence capabilities that provide dedicated intelligence support to committed maneuver units. The overwatch cell is connected via a shared intelligence network that can extract information from multiple sources and provide succinct answers (vice megabytes of information) directly to supported units when time is critical. (FM 2-0) (USAICoE)

Note: This task branch supports ART 6.7 (Conduct Survivability Operations).

No.	*Scale*	*Measure*
01	Yes/No	Selected intelligence Soldiers provided a foundation of regional and subject matter expertise.
02	Yes/No	New intelligence technology was incorporated into the intelligence system.

ART 2.1.4 GENERATE INTELLIGENCE KNOWLEDGE

2-12. Generate intelligence knowledge is a continuous, user-defined task driven by the commander. It begins before mission receipt and provides the relevant knowledge required regarding the operational environment for the conduct of operations. As soon as the intelligence officer and other staff sections begin to collect data on the operational environment, they should organize the data into databases that meet the commander's visualization requirements. The execution of this task must follow all applicable policies and regulations on information collection and operations security. The information and intelligence obtained are refined into knowledge for use in mission analysis through functional analysis. Information is obtained through intelligence reach; research; data mining; database access; academic studies, products, or materials; intelligence archives; open-source intelligence; and other information sources. Generate intelligence knowledge is the foundation for performing intelligence preparation of the battlefield and mission analysis. The primary product of the generate intelligence knowledge task is the initial data files and intelligence survey. (FM 2-0) (USAICoE)

No.	*Scale*	*Measure*
01	Yes/No	Unit obtained detailed information on threat characteristics (composition, disposition, tactics, training, logistics, operational effectiveness, fires, communications, personality, intelligence, reach, agencies, nongovernmental organizations, and other threats) in and affecting the operational environment.
02	Yes/No	Unit obtained detailed information on the types of environment, such as desert, urban, jungle, arctic, and mountain, and the military aspects of terrain.
03	Yes/No	Unit obtained detailed information on recent and historical weather trends, seasonal patterns, aspects of weather, and weather zones in the operational environment. Unit effectively used and integrated the information to determine how the weather potentially affects friendly and enemy forces and operations in the operational environment.
04	Yes/No	Unit obtained detailed information on civil considerations within and affecting the operational environment.
05	Yes/No	Unit used the analytic functions and functional analysis.
06	Yes/No	Unit followed all applicable policies and regulations when collecting information and operations security.

ART 2.1.4.1 DEVELOP THE FOUNDATION TO DEFINE THREAT CHARACTERISTICS

2-13. Obtain detailed information and intelligence concerning threat characteristics (formerly order of battle) affecting the conduct of operations. Obtain this information from sources that include intelligence reach; research; data mining; database access; academic studies, products, or materials; intelligence archives; and open-source intelligence. This task develops specific, detailed information for each threat characteristic. The information, intelligence, products, and materials obtained are refined for use in mission analysis, intelligence preparation of the battlefield (IPB), and other planning tasks. This refinement occurs through functional analysis and other analytic techniques. (FM 2-0) (USAICoE)

No.	Scale	Measure
01	Yes/No	Unit obtained detailed information on composition, disposition, tactics, training, logistics, operational effectiveness, fires, communications, personality, intelligence, reach, agencies, nongovernmental organizations, and other threats in and affecting the operational environment.
02	Yes/No	Information obtained from external agencies, echelons, and partners was adequate for use in mission analysis, IPB, and planning.
03	Yes/No	Information obtained was used and integrated effectively to determine the effects on operations.
04	Percent	Of relevant information obtained from national agencies.
05	Percent	Of relevant information obtained from joint echelons.
06	Percent	Of relevant information obtained from multinational partners.
07	Percent	Of relevant information obtained from higher Army echelons.
08	Percent	Of relevant information obtained from lateral and subordinate echelons.

ART 2.1.4.2 Obtain Detailed Terrain Information and Intelligence

2-14. Obtain detailed information and intelligence about the terrain of the expected area of interest from sources that include intelligence reach; research; data mining; database access; academic studies, products, or materials; intelligence archives; and open-source intelligence. The information, intelligence, products, and material obtained are refined for use in mission analysis, intelligence preparation of the battlefield (IPB), and other planning tasks through functional analysis. This task encompasses the types of environments and the military aspects of terrain. (FM 2-0) (USAICoE)

No.	Scale	Measure
01	Yes/No	Unit obtained detailed information on the types of environment, such as desert, urban, jungle, arctic, and mountain.
02	Yes/No	Information obtained from external agencies, echelons, and partners was adequate for use in mission analysis, IPB, and planning.
03	Yes/No	Information obtained was used and integrated effectively into mission analysis, IPB, and planning.
04	Yes/No	Unit obtained detailed information on the military aspects of terrain.
05	Percent	Of relevant information obtained from national agencies.
06	Percent	Of relevant information obtained from joint echelons.
07	Percent	Of relevant information obtained from multinational partners.
08	Percent	Of relevant information obtained from higher Army echelons.
09	Percent	Of relevant information obtained from lateral and subordinate echelons.

ART 2.1.4.3 Obtain Detailed Weather and Weather Effects Information and Intelligence

2-15. Obtain detailed information and intelligence regarding recent and historical weather trends, seasonal patterns, aspects of weather, and weather zones. Obtain information on how the weather affects friendly and enemy forces and operations in the area of interest Sources of information include intelligence reach; research; data mining; database access via the digital topographic support system; academic studies, products, or materials; intelligence archives; and open-source intelligence. This task requires specific and detailed information for each weather factor. The Integrated Meteorological System (accessed through distributed common groundsystem-Army) provides commanders at all echelons of command with an automated weather system. This system receives, processes, and disseminates weather observations, forecasts, and decision aids for weather and environmental effects to all warfighting functions. The information, intelligence, products, and materials obtained are refined for use in mission analysis, intelligence preparation of the battlefield (IPB), and other planning tasks through functional analysis. (FM 2-0) (USAICoE)

No.	Scale	Measure
01	Yes/No	Unit obtained detailed information the recent and historical weather trends, seasonal patterns, aspects of weather, and weather zones in the operational environment.
02	Yes/No	Information obtained from external agencies, echelons, and partners was adequate for use in mission analysis, IPB, and planning.
03	Yes/No	Information obtained was used and integrated effectively into mission analysis, IPB, and planning.
04	Yes/No	Unit obtained detailed information on each weather factor.
05	Yes/No	Information obtained was used and integrated effectively to determine how the weather affected friendly and enemy forces and operations in the operational environment.
06	Percent	Of relevant information obtained from national agencies.
07	Percent	Of relevant information obtained from joint echelons.
08	Percent	Of relevant information obtained from multinational partners.
09	Percent	Of relevant information obtained from higher Army echelons.
10	Percent	Of relevant information obtained from lateral and subordinate echelons.

ART 2.1.4.4 Obtain Detailed Civil Considerations Information and Intelligence

2-16. Obtain detailed information and intelligence concerning the civil considerations—areas, structures, capabilities, organizations, people, events (ASCOPE)—within or affecting the expected operational environment through reach; research; data mining; database access; academic studies, products, or materials; intelligence archives; open-source intelligence; or other information sources to support operations, planning, execution, and commander's decisions. The data, information, intelligence, products, and material obtained are refined for use in mission analysis, intelligence preparation of the battlefield (IPB), and planning through functional analysis. This task requires specific and detailed information for each ASCOPE factor. This task entails obtaining detailed information and intelligence concerning the civil considerations within or affecting the expected area of interest. The intelligence section obtains this information from sources that include intelligence reach; research; data mining; database access; academic studies, products, or materials; intelligence archives; and open-source intelligence. The data, information, intelligence, products, and materials obtained are refined for use in mission analysis, IPB, and other planning tasks through functional analysis. This task develops specific and detailed information for each characteristic of civil considerations. (FM 2-0) (USAICoE)

Note: This task is supported by ART 2.2.1.5 (Conduct Geospatial Engineering Operations and Functions) and ART 2.2.5 (Conduct Police Intelligence Operations).

No.	Scale	Measure
01	Yes/No	Unit obtained detailed information on areas and structures within and affecting the operational environment.
02	Yes/No	Information obtained from external agencies, echelons, and partners was adequate for use in mission analysis, IPB, and planning.
03	Yes/No	Information obtained was used and integrated effectively into mission analysis, IPB, and planning.
04	Yes/No	Unit obtained detailed information on the capabilities within and affecting the operational environment.
05	Yes/No	Unit obtained detailed information on the organizations, people, and events within and affecting the operational environment.
06	Percent	Of relevant information obtained from national agencies.
07	Percent	Of relevant information obtained from joint echelons.
08	Percent	Of relevant information obtained from multinational partners.

No.	Scale	Measure
09	Percent	Of relevant information obtained from higher Army echelons.
10	Percent	Of relevant information obtained from lateral and subordinate echelons.

ART 2.1.4.5 COMPLETE STUDIES

2-17. To assist in achieving goals and objectives, this task entails providing the requesting command or organization with detailed information, assessments, and conclusions about the area of operations and area of interest. A study can be a systems or functional analysis product. It should be as detailed and in-depth as time allows. Studies provide knowledge that supports understanding of the local populations; cultures and caste system; societal systems or organizations; political systems and structures; religions practiced and their impacts; moral beliefs and their impacts; civil authority considerations; military organizations, structure, and equipment; and attitudes toward U.S., multinational, or host-nation forces. Studies can also include the views and attitudes of multinational and host-nation forces towards these factors. (FM 2-0) (USAICoE)

Note: This task can be conducted in support of ART 2.2 (Support to Situational Understanding).

No.	Scale	Measure
01	Yes/No	Study and conclusions provided commander and staff with necessary information for mission analysis and planning.
02	Yes/No	Unit completed study in time to support mission analysis and planning.
03	Yes/No	Study provided relevant information for mission analysis and planning.
04	Yes/No	Study did not reproduce data contained in readily available publications.
05	Yes/No	Study used maps, charts, and tables to portray data in easily understandable and retrievable formats.
06	Yes/No	Study included, as appropriate, areas (such as historical, religious, or culturally important buildings or landmarks) that could cause a negative view of U.S. forces if attacked or targeted.
07	Yes/No	Study included, as appropriate, industrial infrastructure, natural resources, and areas that may pose environmental or health threat, if attacked.
08	Yes/No	Information for the study was compiled per applicable regulations, policies, and procedures.
09	Yes/No	Unit completed study per applicable regulations, policies, and procedures.
10	Yes/No	Unit spent appropriate amount of time to complete the study.
11	Time	To identify shortfalls and gaps in available data to complete study.
12	Time	To request required data not available from available resources.
13	Percent	Of information requested and received from outside sources.
14	Percent	Of study information, as appropriate, accurate on or concerning the individual topics. Topics can include geography, history, population, culture and social structure, languages, religion, U.S. interests, civil defense, labor, legal, public administration, public education, public finance, public health, public safety, public welfare, civilian supply, civilian economics and commerce, food and agriculture, property control, public communications, public transportation, public works and utilities, arts, monuments, archives, civil information, cultural affairs, dislocated civilians, and host-nation support.

ART 2.1.4.5.1 Conduct Area, Regional, or Country Study of a Foreign Country

2-18. Study and provide mission-focused knowledge of the terrain and weather, civil considerations, and threat characteristics for a specified area or region of a foreign country— including the attitudes of the populace and leaders toward joint, multinational, or host-nation forces—to assist in achieving goals and objectives. Studies can also include the views and attitudes of multinational and host-nation forces. Studies

provide detailed information, assessments, and conclusions on the areas of interest of the requesting command or organization. Studies should be as detailed as time allows. (FM 2-0) (USAICoE)

No.	*Scale*	*Measure*
01	Yes/No	Study provided commander and staff with necessary information for mission analysis and planning.
02	Yes/No	Unit completed study in time to support mission analysis and planning.
03	Yes/No	Study provided relevant information for mission analysis and planning.
04	Yes/No	Study did not reproduce data contained in readily available publications.
05	Yes/No	Study used maps, charts, and tables to portray data in easily understandable and retrievable formats.
06	Yes/No	Study included, as appropriate, areas (such as historical, religious, or culturally important buildings or landmarks) that could cause a negative view of U.S. forces if attacked or targeted.
07	Yes/No	Study included, as appropriate, industrial infrastructure, natural resources, and areas that may pose environmental or health threat, if attacked.
08	Yes/No	Unit spent appropriate time and resources to complete the study.
09	Yes/No	If study was requested from external organization, the request was made to the appropriate external organization.
10	Yes/No	If study was requested from external organization, the study was received in time to support mission analysis and planning.
11	Yes/No	If study was requested from external organization, the study provided relevant information for mission analysis and planning.
12	Yes/No	If study was requested from external organization, the study used maps, charts, and tables to portray data in easily understandable and retrievable formats.
13	Yes/No	If study was requested from external organization, amount and type of information adequate and accurate for the area, region, or country.
14	Yes/No	The initial study was maintained and updated.
15	Yes/No	Information for the study was compiled per applicable regulations, policies, and procedures.
16	Yes/No	Study was completed per applicable regulations, policies, and procedures.
17	Time	To identify shortfalls in available data to complete study.
18	Time	To request required data not available from available resources.
19	Time	Allocated in advance for a study by an external organization prior to mission analysis and planning.
20	Time	Prior to mission analysis and planning that the requested external agency used to deliver the study.
21	Time	From receipt of tasking until study was complete.
22	Percent	Of time available used toward completion of the study.
23	Percent	Of resources available used toward completion of the study.
24	Percent	Of information requested from outside sources provided by those outside sources.

ART 2.1.4.5.2 Conduct Specified Study

2-19. Study and provide focused knowledge of the terrain and weather, civil considerations, and threat characteristics for a specified topic or requirement. Studies provide the requesting command or organization with detailed information, assessments, and conclusions on the area of interest. Studies should be as detailed and in-depth as time allows. (FM 2-0) (USAICoE)

No.	*Scale*	*Measure*
01	Yes/No	Study provided commander and staff with the specified information for mission analysis and planning.
02	Yes/No	Unit completed study in time to support mission analysis and planning.

No.	Scale	Measure
03	Yes/No	Study provided relevant information for mission analysis and planning.
04	Yes/No	Study did not reproduce data contained in readily available publications.
05	Yes/No	Study used maps, charts, and tables to portray data in easily understandable and retrievable formats.
06	Yes/No	Study included, as appropriate, areas (such as historical, religious, or culturally important buildings or landmarks) that could cause a negative view of U.S. forces.
07	Yes/No	Study included, as appropriate, current industrial infrastructure, natural resources, and areas that may pose environmental or health threat.
08	Yes/No	Unit spent appropriate time and resources to complete the study.
09	Yes/No	If study was requested from external organization, the request was made to the appropriate external organization.
10	Yes/No	If study was requested from external organization, the study was received in time to support mission analysis and planning.
11	Yes/No	If study was requested from external organization, the study used maps, charts, and tables to portray data in easily understandable and retrievable formats.
12	Yes/No	If study was requested from external organization, amount and type of information was adequate and accurate for the area, region, or country.
13	Yes/No	The initial study was maintained and updated.
14	Yes/No	Information for the study was compiled per applicable regulations, policies, and procedures.
15	Yes/No	Study was completed per applicable regulations, policies, and procedures.
16	Time	To identify shortfalls in available data to complete study.
17	Time	To request required data not available from available resources.
18	Time	Allocated in advance for a study by an external organization prior to mission analysis and planning.
19	Time	Prior to mission analysis and planning that the requested external agency used to deliver the study.
20	Time	From receipt of tasking until study was complete.
21	Percent	Of time available used toward completion of the study.
22	Percent	Of resources available used toward completion of the study.
23	Percent	Of information requested from outside sources provided by those outside sources.

ART 2.1.5 TAILOR THE INTELLIGENCE FORCE

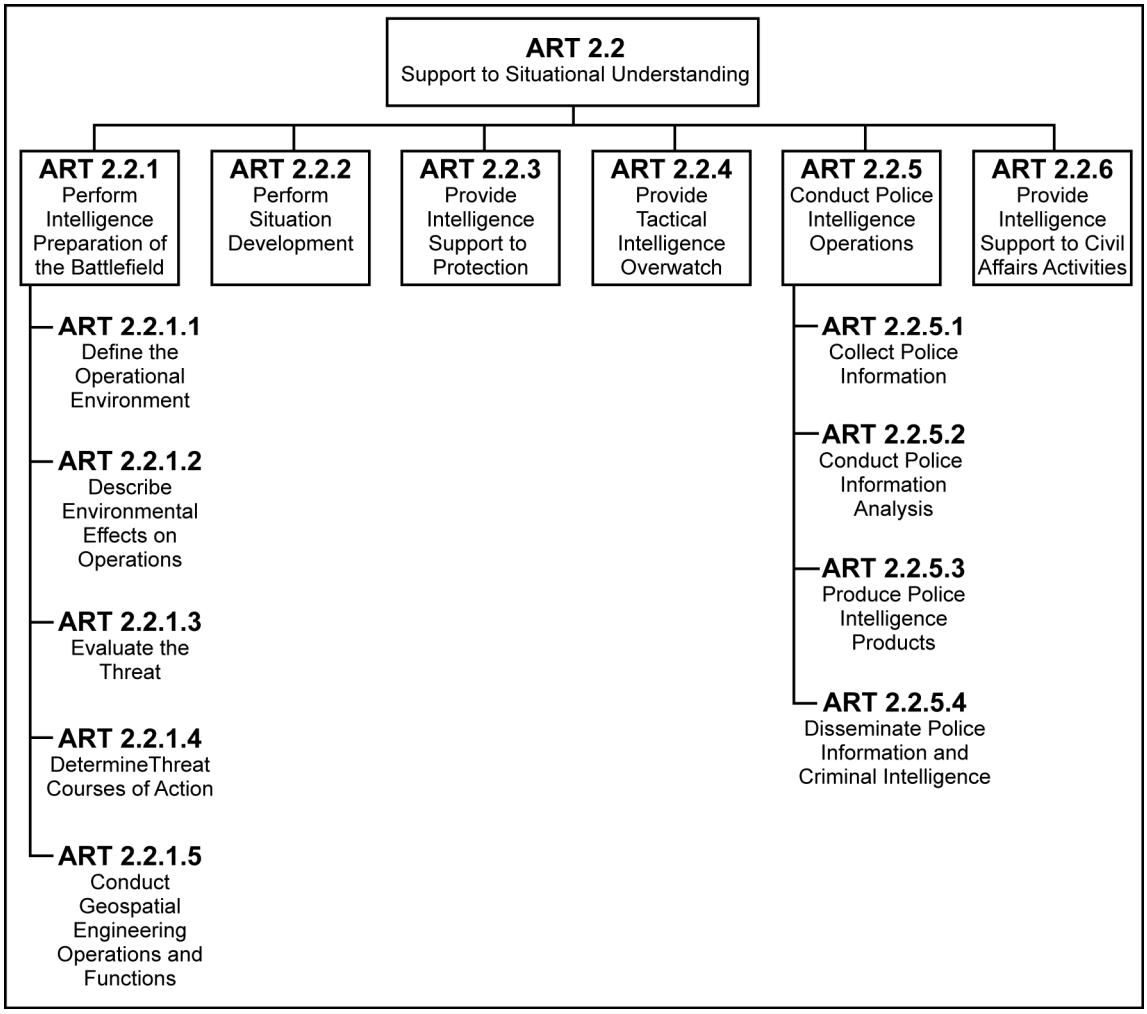
2-20. The generating force uses mission analysis to focus the allocation of intelligence resources for use by a joint task force or combatant commander as well as to support strategic objectives, the Army's mission, and operations at each echelon. Based on their own mission analysis, the staffs at each echelon allocate intelligence resources obtained through the generating force to support the commander's intent, guidance, and mission objectives. (FM 2-0) (USAICoE)

Note: This task supports ART 2.3.1 (Perform Intelligence, Surveillance, and Reconnaissance Synchronization).

No.	Scale	Measure
01	Yes/No	Unit used results of generate knowledge to determine the correct amount intelligence assets required to accomplish the mission.
02	Yes/No	Unit used results of generate knowledge to determine what existing national intelligence requirements need to be reallocated to Army Service component command (ASCC) intelligence services or organizations.

No.	Scale	Measure
03	Yes/No	If the national intelligence requirements were not reallocated, unit requested external intelligence support to accomplish the mission.
04	Yes/No	Unit kept intelligence assets at the ASCC level based on strategic requirements.
05	Yes/No	Unit reallocated intelligence assets to subordinate commanders based on the mission variables.
06	Yes/No	Unit reallocated intelligence assets to subordinate commanders based on operational requirements.
07	Yes/No	Unit reallocated intelligence assets to subordinate echelons as required by the ASCC and corps based on the results from generate knowledge.
08	Yes/No	Unit kept intelligence assets at the corps level based on operational requirements.
09	Yes/No	Intelligence assets allocated to the corps were adequate.
10	Yes/No	Minimum intelligence assets required for the corps mission were reevaluated periodically.
11	Yes/No	Unit reallocated intelligence assets to subordinate commanders based on the current operational environment and requirements.
12	Yes/No	Corps results from generate knowledge were used to determine the minimum intelligence assets required to accomplish the tactical mission.
13	Yes/No	Unit reallocated intelligence assets to subordinate echelons as required based on the corps results from generate knowledge.
14	Yes/No	Intelligence assets were kept at the tactical level commands—divisions, brigades, and battalions—based on tactical requirements.
15	Yes/No	Unit reallocated intelligence assets based on the subordinate commander's area of operation.
16	Yes/No	Intelligence assets allocated to the tactical level commands—divisions, brigades, and battalions—were adequate.
17	Yes/No	Minimum intelligence assets required for the mission were reevaluated periodically.
18	Percent	Of intelligence assets allocated based on the results of generate knowledge.
19	Percent	Of surplus national intelligence requirements reallocated to other intelligence services or organizations.
20	Percent	Of intelligence assets kept at the ASCC level that satisfy only the strategic requirements.
21	Percent	Of intelligence assets reallocated based on operational environment.
22	Percent	Of intelligence assets reallocated based on operational need.
23	Percent	Of intelligence assets allocated to the corps based on the ASCC results from generate knowledge.
24	Percent	Of intelligence assets kept at the corps level that satisfied only the operational requirements.
25	Percent	Of intelligence assets reallocated based on the current operational environment and requirements.
26	Percent	Of intelligence assets reallocated to subordinate units based on tactical need.
27	Percent	Of external intelligence assets received to accomplish the tactical mission.
28	Percent	Of intelligence assets allocated to the tactical level based on the results of corps generate knowledge.
29	Percent	Of intelligence assets were kept at the tactical level commands—divisions, brigades, and battalions—which satisfied only that command's requirements.
30	Percent	Of intelligence assets reallocated based on the subordinate commander's area of operation.
31	Percent	Of intelligence assets reallocated to subordinate units based on tactical requirements.
32	Percent	Of external intelligence assets received to accomplish the mission.

SECTION II – ART 2.2: SUPPORT TO SITUATIONAL UNDERSTANDING



2-21. Support to situational understanding is the task of providing information and intelligence to commanders to assist them in achieving a clear understanding of the force's current state with relation to the threat and other aspects of the AO. It supports the commander's ability to make sound decisions. (FM 2-0) (USAICoE)

No.	*Scale*	*Measure*
01	Yes/No	Unit supported the commander's visualization of the battlefield and situational understanding of the threat.
02	Time	Required to provide intelligence products that facilitate the commander's visualization and situational understanding of the threat.
03	Percent	Of information and intelligence accurate in light of events.
04	Percent	Of information and intelligence requested by commander completed by latest time information and intelligence is of value.
05	Percent	Of produced intelligence judged relevant to military situations.
06	Percent	Of produced intelligence judged timely by users.
07	Percent	Of produced intelligence judged useable by users.

ART 2.2.1 PERFORM INTELLIGENCE PREPARATION OF THE BATTLEFIELD

2-22. Intelligence preparation of the battlefield (IPB) is a systematic process of analyzing and visualizing the portions of the mission variables of threat, terrain and weather, and civil considerations in a specific area of interest and for a specific mission. By applying IPB, commanders gain the information necessary to selectively apply and maximize operational effectiveness at critical points in time and space. IPB is a continuous staff planning activity undertaken by the entire staff. The staff aims to understand the operational environment and the options it presents to friendly and threat forces. (FM 2-01.3) (USAICoE)

No.	*Scale*	*Measure*
01	Yes/No	Products of the IPB process supported the preparation of running estimates and the military decisionmaking process by the supported commander and staff.
02	Yes/No	Unit intelligence staff, with the support of the entire staff, identified characteristics of the area of operations that will influence friendly and threat operations including terrain, civil considerations, weather, and threat considerations.
03	Yes/No	The entire staff, led by the intelligence staff, established limits to the area of interest following the commander's guidance.
04	Yes/No	Unit intelligence staff identified gaps in current intelligence holdings, identified information requirements, and recommended commander's critical information requirements.
05	Yes/No	Unit intelligence staff, with the support of the entire staff, identified characteristics of the battlefield that will influence friendly and threat operations.
06	Yes/No	Unit intelligence staff, with the support of the entire staff, described effects that military actions will have on future operations in the area of operations.
07	Yes/No	Unit intelligence staff, with the support of the entire staff, evaluated the threat.
08	Yes/No	Unit intelligence staff determined the threat course of action.
09	Yes/No	Unit intelligence staff validated templates with updated information.
10	Yes/No	Commander and other unit staff elements in addition to the intelligence staff participated in the process.
11	Yes/No	IPB products assisted the commander's and staff's visualization and decisionmaking.
12	Time	Since IPB products have been updated.
13	Time	To disseminate updated IPB products.
14	Percent	Of produced intelligence judged to be timely (latest time information and intelligence is of value) by users.
15	Percent	Of produced intelligence judged to be accurate in light of events.
16	Percent	Of produced intelligence judged to be useable by users.
17	Percent	Of produced intelligence judged to be complete based upon requests for clarification or expansion.
18	Percent	Of produced intelligence judged to be relevant to the military situation.

ART 2.2.1.1 DEFINE THE OPERATIONAL ENVIRONMENT

2-23. Initially examine the area of operations (AO), define the area of interest, identify other characteristics—such as the role of nongovernmental and international organizations—in the AO that influence friendly and threat operations, and identify gaps in current intelligence holdings. (FM 2-01.3) (USAICoE)

Note: The term "operational" in the title of this task does not refer to the operational level of war.

No.	Scale	Measure
01	Yes/No	Unit operations were delayed, disrupted, or canceled because the staff failed to identify environmental characteristics of the AO.
02	Yes/No	Commander, with the assistance of intelligence staff officer, identified the area of interest.
03	Yes/No	Unit staff identified gaps in current information databases.
04	Yes/No	Public affairs elements accompanied the maneuver brigades and established field media centers to take maximum advantage of these resources.
05	Yes/No	The entire staff identified significant characteristics of the operational environment, to include the status-of-forces agreement, rules of engagement, and other constraints on unit operations.
06	Yes/No	Staff collected and refined their input such as religious, health threat, terrain, meteorological, and hydrological data.
07	Time	To establish or obtain a database that defines the operational environment.
08	Time	Since intelligence preparation of the battlefield products addressing the operational environment have been updated.
09	Time	Required to determine threat characteristics and determine patterns of operations.
10	Percent	Of terrain, meteorological, and hydrological products produced and issued on time to assigned and gained units.
11	Percent	Of information such as religious, health threat, terrain, meteorological, and hydrological data received from higher headquarters or other organizations.
12	Percent	Of accuracy of threat characteristics, to include doctrine, tactics, techniques, and procedures data.
13	Percent	Of accuracy of operational forecasts and products, to include weather effects and terrain trafficability matrices, tide forecasts, light data, and tactical decision aids.
14	Percent	Of hazards in the AO identified and reported to appropriate headquarters.
15	Percent	Of noncombatants in the AO whose location is accurately reported to appropriate headquarters.
16	Percent	Of press coverage and threat propaganda that addresses friendly activities in an AO.
17	Percent	Of the local legal and illegal economy correctly identified in area studies.
18	Percent	Of local decisionmakers and centers of influence correctly identified in area studies. This includes official and unofficial leaders.

ART 2.2.1.2 DESCRIBE ENVIRONMENTAL EFFECTS ON OPERATIONS

2-24. The activity to evaluate all aspects of the area of operations (AO) with which all forces involved —enemy, friendly, and neutral—must contend with during the conduct of full spectrum operations. This includes the portions of the mission variables of terrain, civil considerations, weather, and threat considerations of the AO and the area of interest (FM 2-01.3) (USAICoE)

No.	Scale	Measure
01	Yes/No	Unit operations were delayed, disrupted, or canceled because the staff failed to identify environmental characteristics of the AO.
02	Yes/No	Unit staff identified gaps in current databases.
03	Yes/No	Staff identified and evaluated how terrain affects military operations and the corresponding positive or negative impacts of the operation on the terrain.
04	Yes/No	Staff identified and evaluated how weather affects military operations.
05	Yes/No	Products assisted the commanders and staff's visualization and decisionmaking.
06	Time	To establish or obtain initial operational environment (terrain, civil considerations, weather, and threat considerations) database.
07	Time	Required to evaluate the impact of combat operations and weather on trafficability of the terrain.
08	Time	Since intelligence preparation of the battlefield (IPB) products have been updated.

No.	Scale	Measure
09	Time	To disseminate updated IPB products.
10	Percent	Of analytical products produced and issued on time to assigned and task-organized units.
11	Percent	Of analytical products received from higher headquarters.
12	Percent	Of accuracy of products provided to unit elements.
13	Percent	Of entire staff effort devoted to updating initial operational environment (terrain, civil considerations, weather, and threat considerations) database.
14	Number	Of restrictions on friendly operations resulting from the presence and movement of noncombatants in the AO.

ART 2.2.1.3 EVALUATE THE THREAT

2-25. This activity analyzes current intelligence to determine how the threat normally organizes for combat and conducts operations. The evaluation includes each threat operating system as well as potential criminal organizations, factions, guerrillas, or insurgents. This step focuses on creating threat models and templates that depict how the threat operates when unconstrained by effects of the environment (FM 2-01.3) (USAICoE)

No.	Scale	Measure
01	Yes/No	The threat's capabilities were stated in the intelligence preparation of the battlefield process and accounted for in the military decisionmaking process.
02	Yes/No	Unit used pattern analysis, event analysis, and intelligence from higher headquarters and other organizations to create threat templates, models, and methods of operation and identify high-payoff targets and high-value targets.
03	Yes/No	Unit used Red Team concept to confirm or deny estimates and assessments about threat intentions.
04	Time	Required to incorporate new intelligence data and products into ongoing threat evaluations.
05	Time	To identify threat capabilities and limitations.
06	Time	To update or create threat templates, models, and methods of operation.
07	Time	To disseminate updated threat templates, models, and methods of operation.
08	Percent	Of correctly identified threat templates, models, and methods of operations; capabilities and limitations; high-payoff targets; high-value targets; and threat models.
09	Percent	Of new, processed intelligence integrated to update broad courses of action.

ART 2.2.1.4 DETERMINE THREAT COURSES OF ACTION

2-26. The activity to determine possible threat courses of action (COAs), describe threat COAs, rank COAs in probable order of adoption, and at a minimum identify the most probable and the most dangerous COAs. (FM 2-01.3) (USAICoE)

No.	Scale	Measure
01	Yes/No	The entire staff, under the direction of the intelligence staff, assessed the effects of friendly actions on threat COAs.
02	Yes/No	The threat's likely objectives and desired end state were identified, beginning with the threat command level at one echelon above the friendly unit and ending the process at two echelons below.
03	Yes/No	Unit staff identified opportunities and constraints that the operational environment offers or affords to threat and friendly forces.
04	Yes/No	Unit staff assessed effects of friendly actions on threat COAs.
05	Yes/No	Units considered threat capabilities, effects of the operational environment, and the threat's preference in operations.
06	Yes/No	Units determined most probable and most dangerous COAs and other threat COAs to a micro level of detail as time permitted.

No.	Scale	Measure
07	Yes/No	Units disseminated threat COAs to lower, adjacent, and next higher echelon.
08	Yes/No	Units delivered threat COAs in time to be of value for developing friendly COAs.
09	Yes/No	The G-3 or S-3 led staff war-gaming with full staff participation to validate and update assessments.
10	Time	Required to identify likely threat objectives and desired end states at different threat echelons of command.
11	Time	To identify and analyze the feasibility of each threat COA in terms of time, space, resources, and force ratios required to accomplish its objective.
12	Time	To evaluate and prioritize each identified threat COA.
13	Percent	Of threat branches and sequels correctly identified during planning.
14	Percent	Of new intelligence integrated to update threat COAs.
15	Percent	Of forecasted significant threat actions correctly identified during planning.
16	Percent	Of correctly identified threat high-value targets and tactical centers of mass (before selecting COAs).

ART 2.2.1.5 CONDUCT GEOSPATIAL ENGINEERING OPERATIONS AND FUNCTIONS

2-27. Geospatial engineer operations include functions of terrain analysis, data collection, data generation, database management, data manipulation and exploitation, cartographic production and reproductions, and geodetic survey. Geospatial engineering operations focus on data generation, data management, terrain analysis, and the presentation of their results to the commander. The functions are all interdependent so to prepare a geospatially accurate and timely enabled common operational picture for the commander. (FM 3-34.230) (USAES)

Note: ART 5.3.3 (Facilitate Situational Understanding Through Knowledge Management) includes the processing of sensor data, the interpretation of data into intelligent information, fusion and integration of separate source data, management of the data to include accuracy and data topology, and dissemination of tactical data information. The inclusion of this task does not change the steps of the intelligence preparation of the battlefield process described in FM 2-01.3.

No.	Scale	Measure
01	Yes/No	The availability of accurate geospatial products allowed the commander to deploy and employ the weapon systems effectively.
02	Yes/No	The availability of accurate geospatial products allowed supported commanders and staffs to visualize their areas of operations, interest, and influence.
03	Yes/No	The availability of accurate geospatial products allowed supported commanders and staffs to target enemy systems effectively.
04	Yes/No	The availability of accurate geospatial products allowed supported commanders and staffs to plan air and ground missions efficiently.
05	Yes/No	The availability of accurate geospatial products allowed supported commanders and staffs to counter enemy weapons and intelligence-collection capabilities.
06	Yes/No	The availability of accurate geospatial products supported the commander's and staff's plans to avoid areas.
07	Time	To complete terrain analysis of an area of operations and prepare products supporting intelligence preparation of the battlefield.
08	Time	To complete geodetic survey in the area of operations.
09	Time	To produce and reproduce geospatial information in sufficient quantities to meet supported unit demand.
10	Number	And types of engineer topographic elements available to support unit operations.

ART 2.2.2 PERFORM SITUATION DEVELOPMENT

2-28. Situation development is a process for analyzing information and producing current intelligence concerning the portions of the mission variables of enemy, terrain, and weather, and civil considerations within the area of operations before and during operations. The process helps the intelligence officer recognize and interpret indicators of threat intentions, and objectives. Situation development confirms or denies threat courses of actions (COAs), provides threat locations, explains what the threat is doing in relation to the friendly force commander's intent, and provides an estimate of threat combat effectiveness. The locations and actions of noncombatant elements and nongovernmental organizations in the area of operations that may impact operations should also be considered. Through situation development, the intelligence officer quickly identifies information gaps, explains threat activities in relation to the unit's operations, and assists the commander in gaining and maintaining situational understanding. Situation development helps the commander make decisions, including when to execute branches and sequels. (FM 2-0) (USAICoE)

No.	*Scale*	*Measure*
01	Yes/No	The COA executed by threat forces was predicted during the intelligence preparation of the battlefield process and accounted for in the military decisionmaking process.
02	Yes/No	Threat situation development provided information that helps the commander make decisions to execute branches and sequels.
03	Yes/No	Unit disseminated situation development intelligence to friendly forces.
04	Time	To disseminate situation development intelligence.
05	Time	To produce an updated situation template.
06	Time	To confirm or deny the existing estimate of the threat COA and update the estimate based on current terrain, civil considerations, weather, and threat characteristics.
07	Percent	Of produced intelligence judged accurate based on threat activity.
08	Percent	Of produced intelligence judged complete based on request for clarification or additional information.
09	Percent	Of produced intelligence judged useable to the current situation.
10	Percent	Of produced intelligence judged timely by consumers and users.

ART 2.2.3 PROVIDE INTELLIGENCE SUPPORT TO PROTECTION

2-29. This task includes providing intelligence that supports measures the command takes to remain viable and functional by protecting itself from the effects of threat activities. It also provides intelligence that supports recovery from threat actions. This task supports the protection warfighting function and is linked to antiterrorism and homeland security. (FM 2-0) (USAICoE)

Note: This task branch supports ART 6.7 (Conduct Survivability Operations) and ART 6.6.1 (Identify Potential Terrorist Threats and Other Threat Activities, ART 6.6 Apply Antiterrorism Measures, ART 6.2.5 Support Homeland Security Personnel Recovery Operations).

No.	*Scale*	*Measure*
01	Yes/No	Unit established force protection plan with commander's critical information requirements and reporting channels and requirements.
02	Yes/No	Unit provided information on incidents by threat forces affecting security of the force.
03	Yes/No	Unit provided intelligence support to the antiterrorism program and force protection mission.
04	Yes/No	Intelligence provided to support the antiterrorism program and force protection mission.
05	Percent	Of intelligence relating to potential hostile acts against U.S. forces or installations.
06	Percent	Of intelligence relating to potential criminal acts against U.S. forces or installations.
07	Percent	Of intelligence relating to chemical, biological, radiological, nuclear, and high-yield explosives employment and deployment.

No.	Scale	Measure
08	Percent	Of intelligence to support theater missile defense operations.
09	Percent	Of intelligence relating to threat surveillance and reconnaissance elements.
10	Percent	Of intelligence provided for combatant command to support homeland security or defense.

ART 2.2.4 PROVIDE TACTICAL INTELLIGENCE OVERWATCH

2-30. Tactical intelligence overwatch is creating standing, fixed analytical intelligence capabilities that provide dedicated intelligence support to committed maneuver units. The tactical intelligence overwatch element is connected through a shared intelligence network that can extract information from multiple sources and provide succinct answers directly to supported units when time is critical. (FM 2-0) (USAICoE)

Note: This task branch supports ART 6.7 (Conduct Survivability Operations).

No.	Scale	Measure
01	Yes/No	The tactical intelligence overwatch cell provided succinct information directly to the supported units.
02	Yes/No	Tactical intelligence forces provided a foundation of regional and subject matter expertise.

ART 2.2.5 CONDUCT POLICE INTELLIGENCE OPERATIONS

2-31. Police intelligence operations (PIO) is a military police (MP) function, integrated within all MP operations, which supports the operations process through analysis, production, and dissemination of information collected as a result of police activities to enhance situational understanding, protection, civil control, and law enforcement. Upon analysis, this information may contribute to commander's critical information requirements, intelligence-led, time-sensitive operations, or policing strategies necessary to forecast, anticipate, and preempt crime or related disruptive activities to maintain order. Police intelligence results from the application of systems, technologies, and processes that analyze applicable data and information necessary for situational understanding and focusing policing activities to maintain law and order. (FM 3-19.50) (USAMPS)

Notes: PIO function is not an intelligence discipline; it is a law enforcement function. However, it is within the critical intelligence task, "support situational understanding" that PIO best support the Army operations process and informs the intelligence process. PIO are essential to this task, particularly where irregular threats (criminal, terrorist, and insurgents) threaten the security of U.S. forces and military operations. This function supports and enhances the commander's situational awareness and common operational picture through collection, analysis, and appropriate dissemination of relevant criminal, police information, and police intelligence. PIO are a vital tool of law enforcement and criminal investigators that distributes and focuses military police and criminal investigations assets. U.S. Codes, executive orders, Department of Defense (DOD) directives, and Army regulations contain specific guidance regarding the prohibition of intelligence personnel from collecting intelligence on U.S. citizens, U.S. corporations, and resident aliens. Any access by the intelligence community to information or products resulting from PIO directed against U.S. citizens should undergo competent legal review.

No.	Scale	Measure
01	Yes/No	The conduct of PIO did not violate U.S. Code and applicable DOD and Army regulations against collecting intelligence on U.S. citizens.
02	Yes/No	PIO contributed to reducing criminal activity in the area of operations (AO).
03	Yes/No	Unit updated police intelligence products as additional police and criminal information and related data was collected.

No.	Scale	Measure
04	Yes/No	Unit obtained legal coordination and authorization before using technical listening equipment and technical surveillance equipment.
05	Yes/No	Commander provided list of critical assets to be protected to provost marshal.
06	Yes/No	Unit identified patterns or trends relevant to proactive law and order operations.
07	Yes/No	Military law enforcement received police and criminal information from the host nation.
08	Yes/No	Unit maintained information on known or suspected criminals per regulatory and legal guidance.
09	Yes/No	Unit established activity files, when applicable.
10	Yes/No	Unit established area files, when applicable.
11	Yes/No	Unit safeguarded juvenile records from unauthorized disclosure.
12	Yes/No	Unit established and maintained liaison with host-nation authorities, military and civilian law enforcement agencies, and other organizations as required by the factors of mission, enemy, terrain and weather, troops and support available, time available, civil considerations.
13	Yes/No	Unit provided tactical intelligence obtained to echelon intelligence staff.
14	Yes/No	Unit collected police and criminal information per the intelligence, surveillance, and reconnaissance plan.
15	Yes/No	Unit disseminated police and criminal information to appropriate agencies.
16	Yes/No	Police intelligence requirements and integration were incorporated into the operation plan or order.
17	Yes/No	Police and criminal databases were updated as unit received police and criminal information and data.
18	Time	To determine susceptibility of critical facilities to criminal threat.
19	Time	To identify military resources susceptible to theft and diversion.
20	Time	To identify criminal trends and patterns based upon PIO.
21	Time	To identify trends and patterns by continued association with identified offenders.
22	Time	To develop tactics, techniques, and procedures of operations to assist in eliminating or reducing vulnerability to criminal threat activities.
23	Time	To coordinate with the host nation for police and criminal information.
24	Time	To review internally created police and criminal information to see if information can answer police and criminal information requirements.
25	Time	To coordinate police and criminal information collection by organic assets.
26	Time	To coordinate with staff intelligence officer for required counterintelligence support.
27	Time	To recruit and develop police informants.
28	Percent	Of identified offenders linked to criminal trends.
29	Percent	Of available U.S. police intelligence resources in the AO identified by military law enforcement.
30	Percent	Of criminal-related activities reported by informants prior to their occurrence.
31	Percent	Of terrorist-related activities reported by informants prior to their occurrence.
33	Percent	Of criminal and other potentially disruptive elements in an AO identified before their committing hostile acts against U.S. interests and host-nation elements.

ART 2.2.5.1 COLLECT POLICE INFORMATION

2-32. Collection of police information is a continuous activity. Military police identify gaps in existing police information and develop intelligence requirements. This collection can be completed through several means; military police patrols, police engagement, criminal investigations, collected evidence, database queries and the use of reachback centers. Collection efforts also assist in enhancing protection operations and antiterrorism through identifying potential criminal threats and other threat activities. (FM 3-19.50) (USAMPS)

No.	Scale	Measure
01	Yes/No	The collection of police and criminal information did not violate U.S. Code and applicable Department of Defense and Army regulations against collecting intelligence on U.S. citizens.
02	Yes/No	Police and criminal information collected allowed the unit to prevent or reduce criminal activity in its area of operations (AO).
03	Yes/No	Unit updated police and criminal intelligence products as additional police and criminal information and data was collected.
04	Yes/No	Unit obtained legal coordination and authorization before using technical listening equipment and technical surveillance equipment.
05	Yes/No	Military law enforcement received police and criminal information from the host nation.
06	Yes/No	Unit maintained liaison with host-nation authorities, military and civilian police agencies, and other organizations as required by the factors of mission, enemy, terrain and weather, troops and support available, time available, civil considerations.
07	Yes/No	Unit disseminated police and criminal information to appropriate headquarters and agencies.
08	Yes/No	Unit recruited and developed police informants in the AO.
09	Time	To coordinate with the host nation for police and criminal information.
10	Time	To coordinate police and criminal information collection by organic assets.
11	Time	To coordinate with staff intelligence officer for required counterintelligence support.
12	Time	To develop police and criminal information requirements.
13	Time	To perform law enforcement patrols designed to obtain police and criminal information.
14	Percent	Of known terrorist- or criminal-related activities reported by informants before their occurrence.
15	Percent	Of identified individuals engaged in terrorist- or criminal-related activities reported by informants after their occurrence.
16	Percent	Of criminal and other potentially disruptive elements in an AO identified before they commit hostile acts against U.S. interests and host-nation elements.
17	Percent	Of criminal activities (such as smuggling, vice, counterfeiting, narcotics, extortion, rape, murder, robbery) occurring in an AO identified and reported.
18	Percent	Of AO covered by law enforcement patrols (mounted and dismounted).

ART 2.2.5.2 CONDUCT POLICE INFORMATION ANALYSIS

2-33. Conducting police information analysis is the process that organizes, analyzes, and interprets police information to police intelligence. Police information and intelligence contributes to all-source analysis and the Army operations process. It also assesses police and criminal information to identify trends and patterns of criminal activity. (FM 3-19.50) (USAMPS)

No.	Scale	Measure
01	Yes/No	The police information analysis did not violate U.S. Code and applicable Department of Defense and Army regulations against collecting intelligence on U.S. citizens.
02	Yes/No	The police information analysis allowed the unit to reduce criminal activity in its area of operations (AO).
03	Yes/No	Unit coordinated funds to establish and maintain a police informant operation.
04	Yes/No	Unit identified patterns or trends relevant to proactive law and order operations.
05	Yes/No	Unit analyzed police information and produced actionable criminal intelligence.
06	Yes/No	Unit recruited and developed police informants in the AO.
07	Time	To prepare annex K for provost marshal operation plan and order as required.
08	Time	To identify and assess latest criminal information collected.
09	Time	To identify criminal information resources in the AO.
10	Time	To identify criminal trends and patterns developed in the AO.

No.	Scale	Measure
11	Time	To analyze external criminal information reports.
12	Time	To assess internally created police information.
13	Time	To produce criminal information bulletins and alert notices.
14	Percent	Of criminal priority intelligence requirement collection efforts directed toward subordinate units.
15	Percent	Of available criminal intelligence resources in the AO.
16	Percent	Of known terrorist- and criminal-related activities reported by informants before their occurrence.
17	Percent	Of identified individuals engaged in terrorist- and criminal-related activities reported by informants after their occurrence.
18	Percent	Of accurate reported terrorist- and criminal-related activities.

ART 2.2.5.3 PRODUCE POLICE INTELLIGENCE PRODUCTS

2-34. Police intelligence operations use the intelligence process to produce police intelligence products used by military police leaders. These products focus police operations and contribute to the Army operations process. These products include standardized police information formatted for rapid dissemination, criminal threat assessments based on police information analysis, and assessment and analysis of police capability and capacity. (FM 3-19.50) (USAMPS)

No.	Scale	Measure
01	Yes/No	Developing the police intelligence products did not violate U.S. Code and applicable Department of Defense and Army regulations against collecting intelligence on U.S. citizens.
02	Yes/No	The police intelligence products developed enabled the unit to reduce criminal activity in its area of operations (AO).
03	Yes/No	Unit developed police intelligence products based on police and criminal information collected from external and internal sources.
04	Yes/No	Unit identified patterns or trends relevant to the conduct of proactive law and order operations.
05	Yes/No	Unit produced actionable police intelligence products.
06	Yes/No	Unit disseminated relevant police and criminal intelligence through military law enforcement and civilian and host-nation networks.
07	Yes/No	Products produced were relevant and answered identified police intelligence requirements.
08	Yes/No	Unit provided police information and police intelligence to the military intelligence community within applicable legal constraints.
09	Yes/No	Unit provided support to the police intelligence fusion cell.
10	Time	To identify police and criminal information resources in the AO.
11	Time	To identify criminal trends and patterns developed in the AO.
12	Time	To analyze external police and criminal information reports.
13	Time	To assess internally created police and criminal information.
14	Time	To produce police and criminal information bulletins and alert notices.

ART 2.2.5.4 DISSEMINATE POLICE INFORMATION AND CRIMINAL INTELLIGENCE

2-35. Police information and criminal intelligence is disseminated for use by law enforcement to focus policing activities. Police intelligence products are disseminated and integrated within the operations process enhancing situational understanding, mission planning, and execution at every echelon. These products may be disseminated in support of host-nation law enforcement in combating crime and neutralizing criminal threats to military operations based on trend and pattern analysis and shared with other law enforcement agencies. When legally allowable, these products are provided to the military

intelligence community for fusion and incorporation to the all-source intelligence effort, contributing to a more complete intelligence picture. (FM 3-39) (USAMPS)

Note: The dissemination of police information and criminal intelligence is included in ART 5.8.1 (Conduct Law and Order Operations), ART 5.8.1.1 (Perform Law Enforcement), ART 5.8.1.2 (Conduct Criminal Investigations), ART 5.8.1.6 (Provide Customs Support), ART 4.4 (Conduct Internment and Resettlement Operations), and ART 7.3.2.3 (Perform Host-Nation Police Training and Support). Joint, interagency, and multination coordination is included in ART 5.2.2.1 (Prepare the Command Post for Displacement). (FM 3-39 and FM 3-19.50) (USAMPS)

No.	*Scale*	*Measure*
01	Yes/No	Law enforcement agency personnel investigated offenses against Army forces or property committed by persons subject to military law.
02	Yes/No	Law enforcement agency personnel referred offenses against Army forces or property committed by persons subject to military law.
03	Yes/No	Law enforcement agency personnel monitored all ongoing investigations in the theater of operation.
04	Yes/No	Law enforcement agency personnel received final reports from subordinate elements.
05	Yes/No	Law enforcement agency personnel coordinated with Army Criminal Investigation Command for investigation of all major incidents (deaths, serious bodily injury, and war crimes).
06	Yes/No	Law enforcement agency personnel took control of crime scene.
07	Yes/No	Law enforcement agency personnel identified personnel involved in the crime.
08	Yes/No	A senior law enforcement agency individual formulated an investigative plan.
09	Yes/No	Law enforcement agency personnel processed the crime scene. Processing includes recording investigative notes and sketches, photographing crime scene as necessary, and collecting physical evidence for evaluation.
10	Yes/No	Law enforcement agency personnel released the crime scene to appropriate individuals.
11	Yes/No	Law enforcement agency personnel pursued immediate leads. Pursuing leads includes: interviewing victims and witnesses, obtaining written statements (if appropriate), advising suspects of legal rights, obtaining written statements from suspects, collecting related documents necessary to support specific investigations, and coordinating with the judge advocate office as necessary.
12	Yes/No	Investigators law enforcement agency personnel modified standard interview techniques to overcome any language barriers and cultural differences.
13	Yes/No	Investigators maintained a disciplined and systematic approach in their questioning when doing a long series of interviews on the same basic topic.
14	Yes/No	Law enforcement agency personnel continued the investigation as necessary. Tasks include completing evidence documentation, releasing evidence to evidence custodian, identifying need for crime lab analysis of evidence, obtaining other needed specialized investigative support (polygraph or technical listening equipment), gathering related police intelligence operations from other sources, performing surveillance, submitting status reports, and coordinating investigative efforts and findings with supporting Staff Judge Advocate office.
15	Yes/No	Law enforcement agency personnel closed the case by preparing final report.
16	Time	To complete crime analysis.
17	Percent	Of investigations of minor reported incidents.
18	Percent	Of investigations conducted and reported per AR 195-2.
19	Percent	Of returns on deficient reports of investigations for corrective action or for further investigative activity.
20	Percent	Of crime analysis performed correctly.

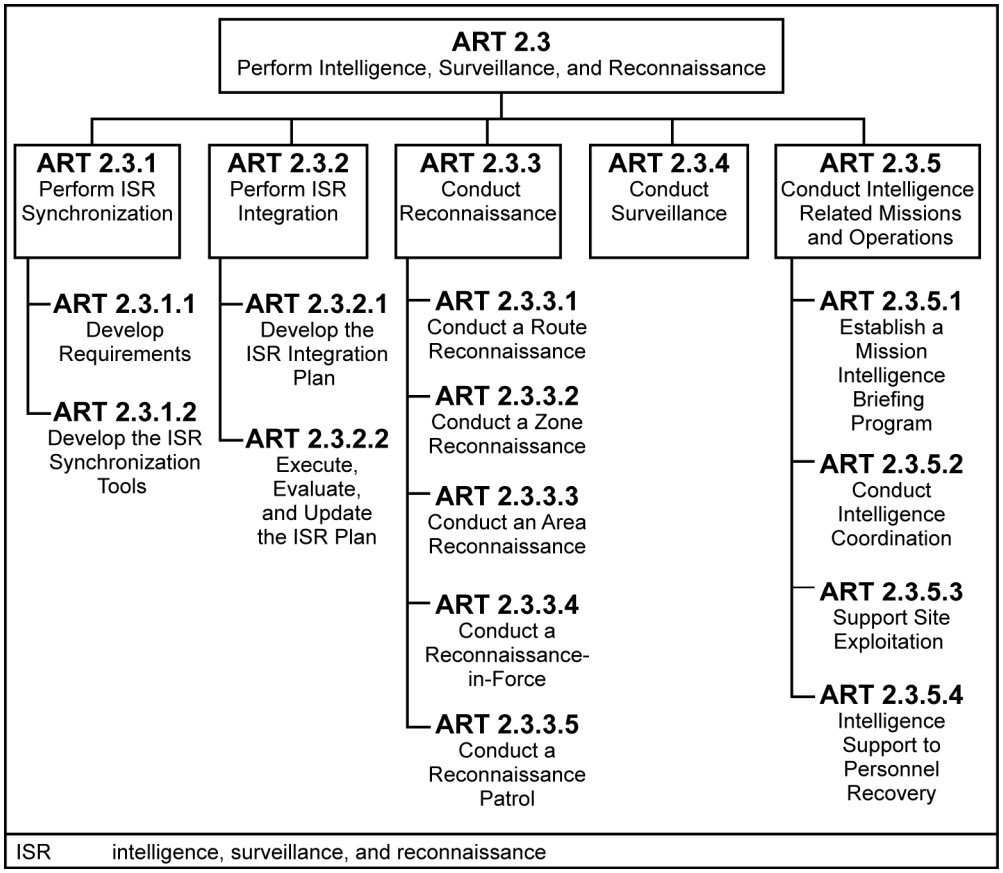
No.	Scale	Measure
21	Percent	Of case documents and required reports prepared per legal, regulatory, and standing operating procedure guidance.
22	Number	Of hotline complaints referred to criminal investigation division or military police investigation.

ART 2.2.6 PROVIDE INTELLIGENCE SUPPORT TO CIVIL AFFAIRS ACTIVITIES

2-36. Military intelligence organizations performing this task collect and provide information and intelligence products concerning civil considerations in support of civil affairs activities. (FM 2-0) (USAICoE)

No.	Scale	Measure
01	Yes/No	Intelligence support required for civil affairs identified through intelligence preparation of the battlefield.
02	Yes/No	Unit provided intelligence information to identify pertinent civil considerations that affect civil affairs operations.
03	Yes/No	Unit provided intelligence support to identify populace perceptions, sentiments, attitudes, mores, allegiances, alliances, and behaviors.
04	Yes/No	Unit provided intelligence support to identify indigenous population and institutions, nongovernmental, and intergovernmental organizations in the area of operations (AO).
05	Yes/No	Unit identified all relevant government agencies, organizations, or departments that effect civil affairs activities.
06	Yes/No	Unit provided intelligence support to identify trends reflected by the national and international media.
07	Yes/No	Unit provided support for to identify resources and capabilities of host-nation population and institutions, nongovernmental, and intergovernmental organizations in the AO.
08	Yes/No	Unit provided intelligence and information to civil affairs within all applicable regulations, policies, and laws.
09	Time	To identify pertinent civil considerations which affect civil affairs activities.
10	Time	To identify populace perceptions, sentiments, attitudes, mores, allegiances, alliances, and behaviors.
11	Time	To identify nongovernmental and international organizations in the AO.
12	Time	To identify all relevant government agencies, organizations, or departments that affect civil affairs activities.
13	Time	To identify trends reflected by the national and international media.
14	Time	To identify resources and capabilities of nongovernmental and international organizations in the AO.
15	Percent	Of accurate information and intelligence provided to civil affairs for civil considerations that affect civil affairs activities.

SECTION III – ART 2.3: PERFORM INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE



2-37. *Intelligence, surveillance, and reconnaissance* is an activity that synchronizes and integrates the planning and operation of sensors, assets, and processing, exploitation, and dissemination systems in direct support of current and future operations. This is an integrated intelligence and operations function. For Army forces, this combined arms operation focuses on priority intelligence requirements while answering the commander's critical information requirements (CCIRs). Through intelligence, surveillance, and reconnaissance (ISR), commanders and staffs continuously plan, task, and employ collection assets and forces. These forces collect, process, and disseminate timely and accurate information, combat information, and intelligence to satisfy the CCIRs and other intelligence requirements. When necessary, ISR assets focus on special requirements, such as personnel recovery. (FM 3-90) (USACAC)

No.	*Scale*	*Measure*
01	Yes/No	Unit developed a strategy to answer each CCIR to accomplish ISR integration.
02	Yes/No	Unit developed requirements that supported the commander's decisionmaking.
03	Yes/No	Unit planned scheme of support including fires, routes of movement and maneuver, air corridors, medical and casualty evacuation, and sustainment.
04	Yes/No	Unit planned for unique support requirements for ISR assets to include maintenance, crew training, downlink nodes, access, and connectivity.
05	Yes/No	Unit developed a detailed ISR plan through a staff process.
06	Yes/No	Unit task-organized ISR forces to perform tasks and accomplish missions.

No.	Scale	Measure
07	Yes/No	Unit developed a debriefing program to capture information observed or gathered by Soldiers (Soldier surveillance and reconnaissance) conducting the ISR operations.
08	Yes/No	Unit satisfied CCIRs using intelligence reach.
09	Yes/No	Unit submitted requests for information to satisfy CCIRs that the commander lacks the organic assets to answer.
10	Yes/No	The operations officer, with the intelligence officer, tasked and directed the available ISR assets to answer the CCIRs.
11	Yes/No	Unit received additional requests from higher headquarters to collect, produce, or disseminate combat information or intelligence products.
12	Yes/No	Unit evaluated each requirement for completion based on reported information.
13	Yes/No	Unit redirected or retasked ISR assets based on reported information.
14	Time	To redirect or retask ISR assets.
15	Percent	Of commander's requirements answered through intelligence reach.
16	Percent	Of commander's requirements answered through requests for information.

ART 2.3.1 PERFORM INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE SYNCHRONIZATION

2-38. *Intelligence, surveillance, and reconnaissance synchronization* is the task that accomplishes the following: analyzes information requirements and intelligence gaps; evaluates available assets internal and external to the organization; determines gaps in the use of those assets; recommends intelligence, surveillance, and reconnaissance (ISR) assets controlled by the organization to collect on the commander's critical information requirements; and submits requests for information for adjacent and higher collection support. (FM 3-0) (USACAC)

Note: This task ensures that ISR, intelligence reach, and requests for information successfully report, produce, and disseminate information, combat information, and intelligence to support decision making. The intelligence officer, in coordination with the operations officer and other staff elements as required, synchronizes the entire collection effort. This effort includes assets the commander controls and those of adjacent and higher echelon units and organizations. It also uses intelligence reach to answer the commander's critical information requirements (CCIRs) and other requirements.

No.	Scale	Measure
01	Yes/No	Unit accomplished ISR synchronization by developing a strategy to answer each priority intelligence requirement (PIR).
02	Yes/No	Unit developed requirements that supported the commander's decisionmaking.
03	Yes/No	Unit determined unique support requirements for ISR assets to include maintenance, crew training, downlink nodes, access, and connectivity.
04	Yes/No	Unit determined scheme of support requirements including fires, routes of movement and maneuver, medical and casualty evacuation, and sustainment.
05	Yes/No	Unit developed and provided ISR task organization recommendations to the operations officer.
06	Yes/No	Unit satisfied CCIRs using intelligence reach and through the request for information (RFI) process.
07	Yes/No	Unit submitted requests for information to satisfy CCIRs that the commander lacks the organic assets to answer.
08	Yes/No	Unit requested collection, products, or dissemination from higher headquarters, adjacent units, or multinational partners to facilitate ISR operations.
09	Yes/No	Unit evaluated each requirement for completion based on reported information.

No.	Scale	Measure
10	Yes/No	Unit delivered the ISR synchronization plan to the operations officer.
11	Yes/No	Unit accomplished ISR synchronization by developing a strategy to answer each PIR.
12	Yes/No	Unit developed requirements that supported the commander's decisionmaking.
13	Percent	Of commander's requirements answered through intelligence reach and through the RFI process.
14	Percent	Of commander's requirements answered through requests for information and through collection, production, or dissemination from higher headquarters.

ART 2.3.1.1 DEVELOP REQUIREMENTS

2-39. The intelligence staff develops a prioritized list focusing on what information it needs to collect to produce intelligence. Additionally, the intelligence staff dynamically updates and adjusts the requirements in response to mission adjustments and changes. Each requirement is assigned a latest time information is of value to meet operational requirements. (FM 2-0) (USAICoE)

No.	Scale	Measure
01	Yes/No	Staff analyzed commander's critical information requirements (CCIRs), including requests for information from lower echelons, adjacent units and organizations, and orders from higher echelons.
02	Yes/No	Unit identified initial intelligence requirements during intelligence preparation of the battlefield.
03	Yes/No	Unit prioritized and validated all information and intelligence requirements by the staff.
04	Yes/No	Commander approved the prioritized and validated requirements developed by the staff.
05	Yes/No	Unit identified mission-specific priority intelligence requirements (PIRs) during the military decisionmaking process course of action (COA) development.
06	Yes/No	Unit performed wargaming for each COA.
07	Yes/No	Unit identified intelligence gaps.
08	Yes/No	Unit developed indicators for each PIR and friendly force information requirements.
09	Yes/No	Unit developed a specific information requirement for each PIR and friendly force information requirement.
10	Time	To validate and incorporate PIR from higher, lower, and adjacent units.
11	Time	Before next phase of an operation when the PIR are validated or updated.
12	Time	Required for the commander to approve the updated PIR.
13	Time	To identify intelligence requirements and if necessary dynamically update or revise in advance of collection.
14	Time	To prioritize information and intelligence collection requirements.
15	Percent	Of PIRs addressed in intelligence update.
16	Percent	Of subordinate echelon requirements supported by the echelon's information and intelligence requirements.
17	Percent	Of invalidated requirements returned to or resubmitted by originating agency or office.
18	Percent	Of validated requirements have ongoing collection efforts directed towards answering requirements.
19	Percent	Of requirements submitted by multiple organizations.
20	Percent	Of PIRs tied to commander's decision points.
21	Percent	Of PIRs linked to specific information requirements.
22	Number	Of open CCIRs and PIRs at any one time.
23	Number	Of requirements identified after collection begins.

ART 2.3.1.2 DEVELOP INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE SYNCHRONIZATION TOOLS

2-40. The entire unit staff develops their information requirements and determines how best to satisfy them. The staff uses surveillance and reconnaissance assets to collect information. There are at least three intelligence, surveillance, and reconnaissance (ISR) synchronization tools: the requirements management matrix, ISR synchronization matrix, and ISR overlay. ISR synchronization tools address all assets the operations officer can task or request as well as the coordinating mechanisms needed to ensure adequate coverage of the area of interest. ISR tools are used to develop the ISR plan. (FM 2-0) (USAICoE)

Note: This task supports ART 2.3.2.1 (Develop the Intelligence, Surveillance, and Reconnaissance Integration Plan)

No.	*Scale*	*Measure*
01	Yes/No	Intelligence officer, with staff participation, used the priority intelligence requirements (PIRs) to begin ISR synchronization.
02	Yes/No	Unit identified all organic, adjacent, and higher echelon ISR assets.
03	Yes/No	Intelligence officer and operations officer, with staff participation, determined asset availability.
04	Yes/No	Unit determined unique support requirements for ISR assets to include maintenance, crew training, downlink nodes, access, and connectivity.
05	Yes/No	Unit developed recommended scheme of support including fires, routes of movement and maneuver, medical and casualty evacuation, and sustainment.
06	Yes/No	Intelligence officer, with staff participation, determined availability and capabilities of assets from higher echelons.
07	Yes/No	Unit identified the reporting criteria, capabilities, limitations, and latest time information is of value for all ISR assets.
08	Yes/No	Unit possessed the right mix of ISR assets for the area of operations.
09	Yes/No	Unit requested additional ISR assets or support when organic assets and attachments cannot provide coverage.
10	Yes/No	ISR synchronization plan addressed redundancy, mix, and cueing.
11	Yes/No	ISR synchronization plan developed and linked to information and intelligence requirements.
12	Yes/No	ISR synchronization plan included the required action or production action needed once requirements were answered.
13	Yes/No	ISR synchronization plan included the reporting procedures and channels for each requirement.
14	Yes/No	Intelligence production answered requirements (specifically PIRs).
15	Yes/No	Unit disseminated ISR synchronization plan to operations officer in time to produce orders and perform troop leading procedures.
16	Time	To determine availability of ISR assets.
17	Time	To develop ISR synchronization plan.
18	Percent	Of requirements identified that is addressed in the ISR synchronization plan.
19	Percent	Of requirements identified that has to be supported by higher echelons.
20	Percent	Of available ISR assets identified.
21	Percent	Of requirements analyzed, validated, and prioritized.

ART 2.3.2 PERFORM INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE INTEGRATION

2-41. *Intelligence, surveillance, and reconnaissance integration* is the task of assigning and controlling a unit's intelligence, surveillance, and reconnaissance assets (in terms of space, time, and purpose) to collect and report information as a concerted and integrated portion of operation plans and orders. Intelligence,

surveillance, and reconnaissance (ISR) integration assigns and controls a unit's ISR assets (in terms of space, time, and purpose) to collect and report information as a concerted and integrated portion of operation plans and orders. The operations officer integrates the best ISR assets through a deliberate and coordinated effort of the entire staff across all warfighting functions into the operation. Specific information requirements facilitate tasking by matching requirements to assets. Intelligence requirements are identified, prioritized, and validated. ISR integration is vital in controlling limited ISR assets. During ISR integration, the staff recommends redundancy, mix, and cue as appropriate. The result of ISR synchronization and integration is an effort focused on answering the commander's requirements. (FM 3-90) (USACAC)

No.	*Scale*	*Measure*
01	Yes/No	ISR plan focused on the commander's critical information requirements.
02	Yes/No	Staff determined unique support requirements for ISR assets to include maintenance, crew training, downlink nodes, access, and connectivity.
03	Yes/No	Staff determined scheme of support including fires, routes of movement and maneuver, medical and casualty evacuation, and sustainment.
04	Yes/No	ISR plan included other staff information requirements.
05	Yes/No	ISR plan provided information and intelligence in time for the commander's decisionmaking.
06	Yes/No	ISR plan included a dissemination plan, to include information tasked or requested from external organizations.
07	Yes/No	Operations officer disseminated ISR plan in time to produce orders and perform troop leading procedures.
08	Yes/No	Staff executed ISR plan.
09	Yes/No	Unit identified indicators of previously unanticipated threat patterns or activities.
10	Yes/No	Unit identified new requirements based on reporting and ISR operations.
11	Yes/No	ISR plan updated and disseminated in time to produce orders.
12	Time	To produce and disseminate initial ISR plan.
13	Time	To evaluate reporting and ISR operations.
14	Time	To determine threat patterns or activities from reporting and ISR operations.
15	Time	To identify indicators of previously unanticipated threat patterns or activities.
16	Time	To review existing information on threat capabilities.
17	Time	To consider threat doctrine.
18	Time	To determine new information and intelligence requirements.
19	Time	To develop new ISR tasks and requests for information.
20	Time	To update and disseminate the ISR plan.
21	Percent	Of specific information and intelligence requirements correctly answered.
22	Percent	Of reporting requirements correctly answered.

ART 2.3.2.1 DEVELOP THE INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE INTEGRATION PLAN

2-42. The operations officer develops the intelligence, surveillance, and reconnaissance (ISR) plan. The entire unit staff analyzes each requirement to determine how best it is to be satisfied. The staff receives ISR tasks and requests for information from subordinate and adjacent units and higher headquarters. The ISR plan includes all assets that the operations officer can task or request and coordinating mechanisms to ensure adequate coverage of the area of interest. (FM 3-90) (USACAC)

No.	*Scale*	*Measure*
01	Yes/No	Intelligence staff provided the operations officer with the ISR synchronization plan.
02	Yes/No	Intelligence staff and operations officer determined asset availability in coordination with the rest of staff.

No.	Scale	Measure
03	Yes/No	All organic, adjacent, and higher ISR assets were tasked against requirements.
04	Yes/No	Staff developed and linked ISR plan to commander and staff requirements.
05	Yes/No	Unit had the right mix of ISR assets for the area of operations.
06	Yes/No	ISR plan addressed redundancy, mix, and cueing.
07	Yes/No	Unit determined unique support requirements for ISR assets to include maintenance, crew training, and connectivity.
08	Yes/No	Unit determined a scheme of support including fires, routes of movement and maneuver, medical and casualty evacuation, and sustainment.
09	Yes/No	Unit identified the reporting criteria, capabilities, and limitations of all ISR assets.
10	Yes/No	Unit linked ISR plan specific information requirements to specific reporting criteria and latest time information is of value.
11	Yes/No	ISR plan provided information and intelligence in sufficient time for the commander's decisionmaking.
12	Yes/No	ISR plan required that ISR forces receive mission intelligence briefing before mission.
13	Yes/No	ISR plan required that ISR assets prepare mission report.
14	Yes/No	ISR plan required that ISR forces are debriefed.
15	Yes/No	ISR plan included a dissemination plan, to include information tasked or requested from external organizations.
16	Yes/No	Operations officer disseminated ISR plan in time to produce operation orders and perform troop leading procedures by subordinates.
17	Yes/No	ISR plan supported the intelligence production and provided answers to requirements.
18	Time	To develop ISR plan.
19	Time	To disseminate the ISR plan.
20	Time	To determine availability of ISR assets.
21	Percent	Of available ISR assets identified.

ART 2.3.2.2 EXECUTE, EVALUATE, AND UPDATE THE INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE PLAN

2-43. The operations officer updates the intelligence, surveillance, and reconnaissance (ISR) plan based on information received from the intelligence officer. The operations officer is the integrator and manager of the ISR effort through an integrated staff process and procedures. As priority intelligence requirements (PIRs) are answered and new information requirements arise, the intelligence officer updates intelligence synchronization requirements and provides the new input to the operations officer who updates the ISR plan. The intelligence and operations officers work closely with all staff elements to ensure the unit's organic collectors receive appropriate taskings. This ISR plan reflects an integrated collection strategy and employment, production, and dissemination scheme that will effectively answer the commander's PIR. This task includes updating ISR operations through dynamic retasking and periodic updates of the ISR plan. (FM 3-90) (USACAC)

No.	Scale	Measure
01	Yes/No	Operations officer disseminated ISR plan in time to produce operation orders and perform troop leading procedures.
02	Yes/No	ISR plan provided information and intelligence in time for the commander to use it in the conduct of the operation.
03	Yes/No	Unit executed ISR plan.
04	Yes/No	ISR assets met latest time information is of value for ISR tasks.
05	Yes/No	ISR assets reported activity or lack of activity in the correct formats and through the required reporting channels.
06	Yes/No	The staff monitored and began evaluation of ISR operations.

No.	Scale	Measure
07	Yes/No	The entire staff conducted analysis of ISR reporting.
08	Yes/No	Unit evaluated reports and identified which requirements had been answered and identified which requirements (PIRs and commander's critical information requirements) to remove.
09	Yes/No	Unit evaluated reports and identified which commander and staff requirements had been satisfied.
10	Yes/No	Unit evaluated reports and identified new requirements.
11	Yes/No	Unit identified gaps or seams within the ISR plan (a continuous measure).
12	Yes/No	Technical authority and channels provided refined information or data to ISR assets.
13	Yes/No	Technical authority and channels provided new technical data to ISR assets.
14	Yes/No	Unit identified indicators of previously unanticipated threat patterns or activities.
15	Yes/No	Unit identified new requirements based on reporting and ISR operations.
16	Yes/No	Unit developed new ISR tasks and requests for information based on new specific information requirements.
17	Yes/No	Dynamic retasking refocused the ISR operation.
18	Yes/No	Operations officer updated and disseminated ISR plan periodically in time to produce operation orders and lead troop movements.
19	Time	To evaluate reporting and ISR operations.
20	Time	To determine threat patterns or activities from reporting and ISR operations.
21	Time	To evaluate and identify gaps or seams within the ISR plan.
22	Time	To identify indicators of previously unanticipated threat patterns or activities.
23	Time	To review existing information on threat capabilities.
24	Time	To consider threat doctrine.
25	Time	To determine new information and intelligence requirements.
26	Time	To develop new ISR tasks and requests for information.
27	Time	To generate and disseminate new ISR tasks as a result of dynamic retasking.
28	Time	To update and disseminate the ISR plan.
29	Percent	Of specific information and intelligence requirements correctly answered.
30	Percent	Of reporting requirements correctly answered.

ART 2.3.3 CONDUCT RECONNAISSANCE

2-44. 2-44. Reconnaissance is a mission undertaken to obtain, by visual observation or other detection methods, information about activities and resources of an enemy or potential enemy and about the meteorological, hydrographic, or geographic characteristics of an area of operations. Other detection methods include signals, imagery, measurement of signature, or other technical characteristics. This task includes performing chemical, biological, radiological, and nuclear reconnaissance; engineer reconnaissance (to include infrastructure reconnaissance and environmental reconnaissance). (FM 3-34.170) (USAIC&FH)

Note: This task branch includes techniques by which ART 6.9.6 may be performed.

No.	Scale	Measure
01	Yes/No	The specific information requirement that prompted the conduct of reconnaissance was answered.
02	Yes/No	Reconnaissance system or force oriented on the intelligence, surveillance, and reconnaissance (ISR) objectives.

No.	Scale	Measure
03	Yes/No	Human intelligence (HUMINT), signals intelligence (SIGINT), imagery intelligence (IMINT), measurement and signature intelligence (MASINT), technical intelligence (TECHINT), and counterintelligence (CI) assets were available for ISR tasking.
04	Yes/No	Reconnaissance system or force reported all information in a timely and accurate manner.
05	Yes/No	Reconnaissance mission completed no later than time specified in the order.
06	Yes/No	Identified support requirements for each reconnaissance asset were sufficient.
07	Yes/No	Available HUMINT, SIGINT, IMINT, MASINT, TECHINT, and CI assets deployed to maximize their capabilities.
08	Yes/No	Unit maintained continuous reconnaissance by employing appropriate asset mix and cueing.
09	Yes/No	Reconnaissance asset was dynamically retasked.
10	Yes/No	Technical authority and channels provided information or data that redirected reconnaissance assets on the ISR objective.
11	Yes/No	Units practiced tactical patience when using HUMINT, SIGINT, IMINT, MASINT, TECHINT, and CI assets.
12	Yes/No	Information observed or gained from contact with the local population (Soldier surveillance and reconnaissance) by units conducting reconnaissance missions was collected by debriefing Soldiers or from unit reports.
13	Yes/No	New tasking received as a result of dynamic retasking.
14	Time	From receipt of tasking until reconnaissance assets are in place and operational.
15	Time	To report information to requesting unit or agency to satisfy priority intelligence requirements (PIR) or information requirements.
16	Time	To redirect or reorient reconnaissance assets to meet new collection requirements.
17	Percent	Of ISR assets collecting against assigned named areas of interest and target areas of interest.
18	Percent	Of PIRs tied to commander's decision points.
19	Percent	Of specific information requirements developed from PIRs.
20	Percent	Of collection requirements fulfilled by reconnaissance assets.
21	Percent	Of accuracy of data provided.
22	Percent	Of reconnaissance mission-capable assets.
23	Percent	Of reconnaissance assets becoming casualties during the mission.

ART 2.3.3.1 CONDUCT A ROUTE RECONNAISSANCE

2-45. Conduct a reconnaissance operation focused along a specific route—such as a road, railway, or waterway—to provide new or updated information on route conditions and activities. (FM 3-90) (USACAC)

No.	Scale	Measure
01	Yes/No	Route reconnaissance accomplished its task or mission, such as determining the trafficability of the route and finding, reporting, and clearing within force capabilities all enemy forces that can influence movement along the route.
02	Yes/No	Reconnaissance force oriented on the reconnaissance objective.
03	Yes/No	Reconnaissance force reported all information rapidly and accurately.
04	Yes/No	Reconnaissance force retained its freedom to maneuver.
05	Yes/No	Reconnaissance force gained and maintained enemy contact.
06	Yes/No	Reconnaissance force rapidly developed the situation.
07	Yes/No	Force reported route reconnaissance critical tasks not performed to higher headquarters.
08	Yes/No	Force accomplished route reconnaissance mission by time specified in the order.

No.	Scale	Measure
09	Yes/No	Force collected information during the route reconnaissance and made it available to the commander.
10	Yes/No	Information observed or gained from contact with the local population (Soldier surveillance and reconnaissance) by units conducting route reconnaissance was collected by debriefing Soldiers or from unit reports.
11	Time	From receiving task until unit reconnaissance assets are in place.
12	Time	To provide collected route data to tasking agency analysts.
13	Time	To redirect reconnaissance assets to meet new requirements.
14	Time	From receiving task until completing route reconnaissance.
15	Percent	Of route reconnaissance critical tasks fulfilled by reconnaissance assets.
16	Percent	Of tactical-level requirements satisfied by higher or adjacent units' existing intelligence, surveillance, and reconnaissance assets on a noninterference basis.
17	Percent	Of accuracy of data provided.
18	Percent	Of operational assets committed to the route reconnaissance mission.
19	Percent	Of reconnaissance assets becoming casualties during the mission.

ART 2.3.3.2 CONDUCT A ZONE RECONNAISSANCE

2-46. Conduct a directed effort to obtain detailed information about all routes, obstacles (to include chemical, biological, radiological, and nuclear contamination), terrain, and enemy forces in an area defined by boundaries. The commander normally assigns a zone reconnaissance when the enemy situation is vague or when information concerning cross-country trafficability is desired. (FM 3-90) (USACAC)

No.	Scale	Measure
01	Yes/No	Zone reconnaissance accomplished its task or mission, such as finding and reporting all enemy forces in the designation area and clearing all enemy forces in the designated area of operations (AO).
02	Yes/No	Human intelligence (HUMINT), signals intelligence (SIGINT), imagery intelligence (IMINT), measurement and signature intelligence (MASINT), technical intelligence (TECHINT), and counterintelligence (CI) assets were available for intelligence, surveillance, and reconnaissance (ISR) tasking.
03	Yes/No	Reconnaissance force was oriented on the reconnaissance objective.
04	Yes/No	Reconnaissance force reported all information rapidly and accurately.
05	Yes/No	Reconnaissance force retained its freedom to maneuver.
06	Yes/No	Reconnaissance force gained and maintained enemy contact.
07	Yes/No	Reconnaissance force rapidly developed the situation.
08	Yes/No	Reported zone reconnaissance tasks performed to higher headquarters.
09	Yes/No	Unit cleared the AO that defines the zone of all enemy forces within the capability of the unit performing the zone reconnaissance.
10	Yes/No	Unit accomplished zone reconnaissance mission by time specified in the operation order.
11	Yes/No	Unit deployed available HUMINT, SIGINT, IMINT, MASINT, TECHINT, and CI assets to maximize their capabilities.
12	Yes/No	Unit practiced tactical patience when using HUMINT, SIGINT, IMINT, MASINT, TECHINT, and CI assets.
13	Yes/No	Information observed or gained from contact with the local population (Soldier surveillance and reconnaissance) by units conducting a zone reconnaissance was collected by debriefing Soldiers or from unit reports.
14	Time	From receiving task until unit reconnaissance assets are in place.
15	Time	To provide collected data to tasking agency analysts.
16	Time	To redirect reconnaissance assets to meet new requirements.
17	Time	From receiving task until completing zone reconnaissance.

No.	Scale	Measure
18	Percent	Of assigned zone reconnaissance tasks fulfilled by reconnaissance assets.
19	Percent	Of tactical-level requirements satisfied by higher or adjacent units' existing ISR assets on a noninterference basis.
20	Percent	Of accuracy of data provided.
21	Percent	Of zone reconnaissance mission-capable assets.
22	Percent	Of reconnaissance assets becoming casualties during the mission.

ART 2.3.3.3 CONDUCT AN AREA RECONNAISSANCE

2-47. Conduct a directed effort to obtain detailed information concerning the terrain or enemy activity within a prescribed area not defined by boundaries, such as a town, ridgeline, woods, or other feature critical to operations to include underwater reconnaissance, search, or recovery. (FM 3-90) (USACAC)

No.	Scale	Measure
01	Yes/No	Area reconnaissance accomplished its task or mission, such as finding and reporting all enemy forces within the designation area and clearing all enemy forces in the designated area of operations (AO) within the capability of the unit conducting reconnaissance.
02	Yes/No	Human intelligence (HUMINT), signals intelligence (SIGINT), imagery intelligence (IMINT), measurement and signature intelligence (MASINT), technical intelligence (TECHINT), and counterintelligence (CI) assets were available for intelligence, surveillance, and reconnaissance (ISR) tasking.
03	Yes/No	Reconnaissance force oriented on the reconnaissance objective.
04	Yes/No	Reconnaissance force reported all information rapidly and accurately.
05	Yes/No	Reconnaissance force retained its freedom to maneuver.
06	Yes/No	Reconnaissance force gained and maintained enemy contact.
07	Yes/No	Reconnaissance force rapidly developed the situation.
08	Yes/No	Reported area reconnaissance tasks not performed to higher headquarters.
09	Yes/No	Unit cleared AO that defined the area of all enemy forces within the capability of the unit performing the area reconnaissance.
10	Yes/No	Unit accomplished area reconnaissance mission by time specified in the order.
11	Yes/No	Unit deployed available HUMINT, SIGINT, IMINT, MASINT, TECHINT, and CI assets in a manner to maximize their capabilities.
12	Yes/No	Unit practiced tactical patience when using HUMINT, SIGINT, IMINT, MASINT, TECHINT, and CI assets.
13	Yes/No	Information observed or gained from contact with the local population (Soldier surveillance and reconnaissance) by units conducting an area reconnaissance was collected by debriefing Soldiers or from unit reports.
14	Time	From receiving task until unit reconnaissance assets are in place.
15	Time	To provide collected data to tasking agency analysts.
16	Time	To redirect reconnaissance assets to meet new requirements.
17	Time	From receiving task until completing area reconnaissance.
18	Percent	Of assigned area reconnaissance tasks fulfilled by reconnaissance assets.
19	Percent	Of tactical-level requirements satisfied by higher or adjacent units' existing ISR assets on a noninterference basis.
20	Percent	Of accuracy of data provided.
21	Percent	Of area reconnaissance mission-capable assets.
22	Percent	Of reconnaissance assets becoming casualties during the mission.

ART 2.3.3.4 CONDUCT A RECONNAISSANCE-IN-FORCE

2-48. A reconnaissance in force is a deliberate combat operation designed to discover or test the enemy's strength, dispositions, and reactions or to obtain other information. (FM 3-90) (USACAC)

No.	*Scale*	*Measure*
01	Yes/No	Reconnaissance-in-force accomplished its task or mission, such as penetrating the enemy's security area, determining its size and depth, and determining the location and disposition of enemy main positions.
02	Yes/No	Unit conducting the reconnaissance-in-force remained oriented on the reconnaissance objective.
03	Yes/No	Unit conducting the reconnaissance-in-force reported all information rapidly and accurately to its higher headquarters.
04	Yes/No	Unit conducting the reconnaissance-in-force retained its freedom to maneuver.
05	Yes/No	Unit conducting the reconnaissance-in-force gained and maintained enemy contact.
06	Yes/No	Unit conducting the reconnaissance-in-force rapidly developed the situation.
07	Yes/No	Unit conducting the reconnaissance-in-force reported reconnaissance-in-force tasks not performed to higher headquarters.
08	Yes/No	Unit completed the reconnaissance-in-force by time specified in the order.
09	Yes/No	Unit collected desired information during the reconnaissance-in-force and made it available to the commander.
10	Yes/No	Information observed or gained from contact with the local population (Soldier surveillance and reconnaissance) by units conducting a reconnaissance in force was collected by debriefing Soldiers or from unit reports.
11	Time	From receiving task until unit reconnaissance assets are in place.
12	Time	To provide collected data to tasking agency analysts.
13	Time	To redirect reconnaissance assets to meet new requirements.
14	Time	From receiving task until completing reconnaissance-in-force.
15	Percent	Of doctrinal reconnaissance-in-force tasks fulfilled by reconnaissance assets.
16	Percent	Of tactical-level requirements satisfied by higher or adjacent units' existing intelligence, surveillance, and reconnaissance assets on a noninterference basis.
17	Percent	Of accuracy of data provided.
18	Percent	Of unit assets mission capable at different points during the reconnaissance-in-force mission—beginning, end, and critical times.
19	Percent	Of unit Soldiers becoming casualties during the mission.

ART 2.3.3.5 CONDUCT A RECONNAISSANCE PATROL

2-49. Use a detachment of ground, sea, or air forces to gather information about the enemy, terrain, or civil environment. (FM 3-90) (USACAC)

No.	*Scale*	*Measure*
01	Yes/No	Patrol collected the information required.
02	Yes/No	Unit prepared patrol plan within time allowed.
03	Yes/No	Unit conducted rehearsals to standard within the time allowed.
04	Yes/No	Patrol used tactically appropriate reconnaissance tactic—fan, converging route, or successive bounds.
05	Yes/No	Enemy detected reconnaissance patrol.
06	Yes/No	Information observed or gained from contact with the local population (Soldier surveillance and reconnaissance) by units conducting a reconnaissance patrol was collected by debriefing Soldiers or from unit reports.
07	Time	To conduct the reconnaissance patrol by time allocated by higher headquarters.
08	Percent	Of assigned area covered during the patrol.

No.	Scale	Measure
09	Percent	Of tactical-level requirements satisfied by higher or adjacent units' existing intelligence, surveillance, and reconnaissance assets on a noninterference basis.
10	Percent	Of accuracy of data provided.
11	Percent	Of friendly casualties received during the combat patrol.
12	Percent	Of information requirements achieved.

ART 2.3.4 CONDUCT SURVEILLANCE

2-50. *Surveillance* is the systematic observation of aerospace, surface, or subsurface areas, places, persons, or things by visual, aural, electronic, photographic, or other means. (JP 3-0) Other means may include but are not limited to space-based systems, and special chemical, biological, radiological, and nuclear; artillery; engineer; special operations forces; and air defense equipment. Surveillance involves observing an area to collect information. (FM 2-0) (USAICoE)

No.	Scale	Measure
01	Yes/No	Surveillance assets collected required information.
02	Yes/No	Identified support requirements for each surveillance asset was sufficient.
03	Yes/No	Human intelligence (HUMINT), signals intelligence (SIGINT), imagery intelligence (IMINT), measurement and signature intelligence (MASINT), technical intelligence (TECHINT), and counterintelligence (CI) assets were available for intelligence, surveillance, and reconnaissance tasking.
04	Yes/No	Unit deployed available HUMINT, SIGINT, IMINT, MASINT, TECHINT, and CI assets to maximize their capabilities.
05	Yes/No	Enemy forces detected surveillance asset.
06	Yes/No	Surveillance system or force reported all information in a timely and accurate manner.
07	Yes/No	Unit maintained continuous surveillance by using appropriate asset mix and cueing.
08	Yes/No	Unit practiced tactical patience when using HUMINT, SIGINT, IMINT, MASINT, TECHINT, and CI assets.
09	Yes/No	Information observed or gained from contact with the local population (Soldier surveillance and reconnaissance) by units conducting a surveillance mission was collected by debriefing Soldiers or from unit reports.
10	Time	From receipt of tasking until surveillance assets are in place and operational.
11	Time	To respond to new taskings.
12	Time	To provide collected data to tasking agency analysts.
13	Time	To report information to requesting unit or agency to satisfy priority intelligence requirements or information requirements.
14	Percent	Of time able to respond to collection requirements.
15	Percent	Of collection requirements fulfilled by surveillance assets.
16	Percent	Of surveillance requirements satisfied using intelligence reach.
17	Percent	Of surveillance assets mission capable.
18	Percent	Of surveillance assets becoming casualties during the mission.
19	Percent	Of assets collecting against assigned named areas of interest and target areas of interest.

ART 2.3.5 CONDUCT INTELLIGENCE RELATED MISSIONS AND OPERATIONS

2-51. The associated intelligence tasks (mission and debriefing program, intelligence coordination, technical authority, and intelligence support to personnel recovery) that facilitate the conduct of reconnaissance and surveillance. It also includes specialized missions (such as sensitive site exploitation), that provide intelligence and information outside of the traditional ISR construct. (FM 2-0) (USAICoE)

ART 2.3.5.1 ESTABLISH A MISSION INTELLIGENCE BRIEFING AND DEBRIEFING PROGRAM

2-52. Commanders establish, support, and allocate appropriate resources for a mission briefing and debriefing program. Conducting battle updates and after action reviews are separate tasks from the mission briefing and debriefing program. The intelligence officer develops a mission intelligence briefing plan and complementary debriefing plan to support the commander's program. Soldiers receive a mission intelligence briefing before executing a patrol or similar operation. The briefing sensitizes Soldiers to specific information and reporting requirements, information gaps, and unique mission requirements. The mission intelligence briefings and debriefings generally follow the format of a mission briefing: review the route traveled, collection objectives of the patrol, and methods employed. The debriefing program captures the specific information requirements the patrol was to collect and any additional information and observations the patrol made concerning the operational environment. It also collects any fliers, pamphlets, media, or pictures the patrol found or obtained. (FM 2-0) (USAICoE)

No.	*Scale*	*Measure*
01	Yes/No	Command established and supported a mission briefing and debriefing program.
02	Yes/No	Command allocated appropriate resources (time, personnel, and a designated area) to support the mission briefing and debriefing program.
03	Yes/No	Units performed battle update briefing and after action reviews separately from the mission briefing and debriefing program.
04	Yes/No	G-2 or S-2 developed a mission intelligence plan.
05	Yes/No	G-2 or S-2 allocated resources for the mission briefing.
06	Yes/No	G-2 or S-2 developed a complementary debriefing plan.
07	Yes/No	G-2 or S-2 allocated resources for the debriefing.
08	Time	That command allocated to mission briefings and debriefings.
09	Time	That G-2 or S-2 allocated for mission intelligence briefing.
10	Time	That G-2 or S-2 allocated to conduct debriefings.

ART 2.3.5.1.1 Establish a Mission Intelligence Briefing Plan

2-53. The intelligence section develops a mission intelligence briefing plan. The mission intelligence briefing plan identifies information Soldiers executing patrols should be seeking. It ensures that all Soldiers conducting patrols, tactical movements, and nontactical movements are sensitized to specific information and reporting requirements, information gaps, and unique mission requirements. The intelligence mission briefing and debriefing generally follow the format of a mission briefing: review the route traveled, collection objectives of the patrol, and methods employed. (FM 2-0) (USAICoE)

No.	*Scale*	*Measure*
01	Yes/No	All patrols, tactical movements, and nontactical movements received mission intelligence briefing.
02	Yes/No	Mission intelligence briefing contained terrain impacts update.
03	Yes/No	Mission intelligence briefing contained civil considerations update.
04	Yes/No	Mission intelligence briefing contained weather effects update.
05	Yes/No	Mission intelligence briefing contained threat update.
06	Yes/No	Mission intelligence briefing contained route update.
07	Yes/No	Mission intelligence briefing contained focus areas for observation.
08	Yes/No	Mission intelligence briefing contained updated collection requirements.
09	Yes/No	Mission intelligence briefing provided criteria for immediate reporting requirements.
10	Yes/No	Mission intelligence briefing provided reporting requirements for nonpriority reporting.
11	Yes/No	Mission briefing contained reporting requirements for unusual activity or complete lack of activity by the local population.
12	Yes/No	Mission briefing contained requirements for handling and disposing collected documents.

No.	Scale	Measure
13	Yes/No	Mission briefing contained requirements for enemy prisoner of war and detainee and captured enemy document handling and disposition.
14	Yes/No	Mission intelligence briefing contained requirements for use of digital photography.

ART 2.3.5.1.2 Establish a Debriefing Plan

2-54. The intelligence section develops a complementary debriefing plan. The debriefing plan captures information related to the specific information requirements the patrol was to collect and any additional information and observations the patrol made concerning the operational environment. It also collects any fliers, pamphlets, media, or pictures the patrol found or obtained. The plan should include all returning patrols, leaders who have traveled to meetings, returning human intelligence collection teams, aircrews, and others who may have obtained information of intelligence value. The intelligence section debriefs personnel. Debriefers then write and submit a report or reports information verbally, as appropriate. The requirement for a debriefing by the intelligence section following each mission should be a part of the intelligence mission briefing. Leaders should not consider the mission complete and release the personnel until the reporting and debriefings are done. (FM 2-0) (USAICoE)

No.	Scale	Measure
01	Yes/No	Units attended and participated in all patrols, tactical movements, and nontactical movements in postmission intelligence debriefing upon return.
02	Yes/No	Units completed and submitted mission reports for all patrols, tactical movements, and nontactical movements upon return.
03	Yes/No	Debriefing conducted in a logical and organized manner.
04	Yes/No	Debriefing conducted with all members of the patrols, tactical movements, and nontactical movements.
05	Yes/No	Debriefing addressed information pertaining to the tasked collection requirements.
06	Yes/No	Debriefing addressed additional details on information provided through immediate reporting during the mission or movement.
07	Yes/No	Debriefing addressed information provided through nonpriority reporting during the mission or movement.
08	Yes/No	Debriefing addressed unusual activity or complete lack of activity by the local population observed during the mission or movement.
09	Yes/No	Debriefing addressed documents found or photographed during the mission or movement.
10	Yes/No	Debriefing addressed enemy prisoner of war and detainee encountered during the mission.
11	Yes/No	Debriefing addressed any conversations unit members had with the local populace.

ART 2.3.5.2 CONDUCT INTELLIGENCE COORDINATION

2-55. Conduct intelligence coordination is the task carried out by the intelligence section to facilitate active collaboration, laterally and vertically. It includes establishing and maintaining technical channels to refine and focus the intelligence disciplines in intelligence, surveillance, and reconnaissance (ISR) tasks. It also properly coordinates the discipline assets when operating in another unit's area of operations (AO). (FM 2-0) (USAICoE)

No.	Scale	Measure
01	Yes/No	Technical authority and channels capability and expertise resided in the G-2 or S-2.
02	Yes/No	Units used technical authority and channels to train assets before the mission.
03	Yes/No	Units used technical authority and channels to identify, define clearly, and disseminate the legal limits of how to use specific ISR assets.
04	Yes/No	Units handled technical information and guidance to support operations following all applicable regulations, policies, and procedures.
05	Yes/No	Intelligence assets and units coordinated with friendly units when entering, moving through, or departing friendly lines or areas of operations.

No.	Scale	Measure
06	Yes/No	Units monitored the technical authority and channels of operations to ensure missions conducted within applicable regulations, policies, and procedures; provided control measures for ISR synchronization effort; and ensured a collaborative collection and information environment.
07	Yes/No	Intelligence assets and units identified specific offices for liaison to exchange relevant information and intelligence with the friendly units.

ART 2.3.5.2.1 Establish and Maintain Technical Authority and Channels

2-56. Intelligence commanders and intelligence staffs maintain control of each intelligence discipline during operations through technical channels to ensure adherence to applicable laws and policies, ensure proper use of doctrinal techniques, and provide technical support and guidance. Applicable laws and policies include all relevant U.S. law, the law of war, international law, directives, DOD instructions, and orders. Commanders direct operations but often rely on the intelligence section's technical expertise to conduct portions of the unit's collection effort. Technical channels also involve translating ISR tasks into the specific parameters used to focus highly technical or legally sensitive aspects of the intelligence, surveillance, and reconnaissance (ISR) effort. Technical channels include but are not limited to defining, managing, or guiding the use of specific ISR assets; identifying critical technical collection criteria, such as technical indicators; recommending collection techniques, procedures, or assets; coordinating operations; and directing specialized training for specific MI personnel or units. (FM 2-0) (USAICoE)

Note. In specific cases, regulatory authority is granted to specific national and DOD intelligence agencies for specific intelligence discipline collection and is passed through technical channels.

No.	Scale	Measure
01	Yes/No	Technical authority and channels capability and expertise resided within the G-2 or S-2.
02	Yes/No	Unit requested technical authority and channel capability as well as resident expertise if it was not resident within the G-2 or S-2.
03	Yes/No	Unit used technical authority and channels to train assets before the mission.
04	Yes/No	Unit conducted operations per all applicable regulations, policies, and procedures, to include classification and security considerations.
05	Yes/No	Unit used technical authority and channels to identify, define clearly, and disseminate the legal limits of the use of specific ISR assets.
06	Yes/No	Unit handled technical information and guidance to support operations per all applicable regulations, policies, and procedures.
07	Yes/No	Unit monitored technical authority and channels to ensure missions conducted within applicable regulations, policies, and procedures.
08	Yes/No	Technical authority and channels reported operations and missions that violated applicable regulations, policies, and procedures.
09	Yes/No	Unit used technical authority and channels to determine what existing national intelligence assets or higher echelon Army assets were satisfying requirements that allow organic assets to be reallocated for other missions.
10	Yes/No	Unit used technical authority and channels to determine the minimum intelligence assets required for the mission periodically reevaluated.
11	Yes/No	Technical authority and channels provided technical guidance and control measures to the G-2 or S-2 for ISR synchronization efforts.
12	Yes/No	Technical channels provided the commander information and intelligence to support lethal and nonlethal targeting of the threat.
13	Yes/No	Technical authority and channels monitored and identified all technical control measures to ensure unit met reporting criteria.
14	Yes/No	Technical authority and channels ensured a collaborative collection and information environment for all available intelligence disciplines.

No.	Scale	Measure
15	Yes/No	Technical controls ensured continuous technical interface between all applicable ISR assets.
16	Yes/No	G-2 or S-2 section monitored ISR collection and compared it to the event template and matrix to determine if the technical authority and channels were meeting predicted course of action requirements.
17	Time	To identify, define, and disseminate the legal limits using technical authority and channels.
18	Time	To provide information and guidance to support operations using technical authority and channels.
19	Percent	Of technical guidance and control measures given to the G-2 or S-2 for ISR synchronization efforts.

ART 2.3.5.2.2 Conduct Deconfliction and Coordination

2-57. Deconfliction and coordination consists of a series of related activities that facilitate operations in another unit's area of operations (AO). These activities facilitate successful intelligence, surveillance, and reconnaissance collection, support of the operation, and fratricide avoidance. Military intelligence organizations may be used in general support for coverage of an AO or in direct support to support a specific unit. Military intelligence organizations operating in general support should coordinate with unit commanders when operating in that unit's AO. At a minimum, the military intelligence organizations announce their presence and request information on any conditions or ongoing situations that may affect how they conduct their mission—organizations should conduct thorough face-to-face coordination. A military intelligence organization operating in direct support of a specific unit coordinates with the unit for augmentation to conduct operations in accordance with force protection requirements. The military intelligence organization's leader also coordinates with the supported unit's intelligence section for debriefings of returning members, convoy leaders, and others. (FM 2-0) (USAICoE)

No.	Scale	Measure
01	Yes/No	Intelligence assets and units conducted coordination with friendly units when entering, moving through, or departing friendly lines or AOs.
02	Yes/No	Intelligence assets and units provided a liaison with the friendly forward unit, when available.
03	Yes/No	Intelligence assets and units coordinated with the friendly forward unit within whose AO they would be operating for exchanged graphics and overlays; fire support (en route, at mission location, and return); casualty evacuation procedures; passwords (running, forward of friendly lines); recognition signals, call signs, and frequencies; approved routes for movement; off-limits or restricted areas; maintenance and resupply points; reporting criteria to share relevant information and intelligence; and key information concerning the operational environment.
04	Yes/No	Intelligence assets and units exchanged relevant information and intelligence with the friendly forward unit.

ART 2.3.5.3 SUPPORT SITE EXPLOITATION

2-58. *Site exploitation* consists of a related series of activities inside a captured sensitive site to exploit personnel, documents, electronic data, and material captured at the site, while neutralizing any threat posed by the site or its contents. A sensitive site is a designated, geographically limited area with special diplomatic, informational, military, and economic sensitivity for the United States. This includes factories with technical data on enemy weapon systems, war crimes sites, critical hostile government facilities, areas suspected of containing persons of high rank in a hostile government or organization, terrorist money laundering areas, and document storage areas for secret police forces. While the physical process of exploiting the sensitive site begins at the site itself, full exploitation may involve teams of experts located around the world. (FM 3-90.15) (USACAC)

No.	Scale	Measure
01	Yes/No	Exploitation of the sensitive site supported U.S. operational or strategic diplomatic, informational, military, and economic goals.
02	Yes/No	Unit supporting the exploitation of the sensitive site had isolated, seized, secured, and cleared the site or relieved a unit that accomplished those tactical missions prior to exploiting the site under the technical direction of subject matter experts.
03	Yes/No	Enemy or adversary knew that U.S. forces had exploited the site.
04	Yes/No	Tactical unit task organized itself appropriately to accomplish the mission of supporting the exploitation of the sensitive site and compensated for losses.
05	Yes/No	Enemy or adversary failed to exfiltrate sensitive equipment or materiel from the sensitive site.
06	Yes/No	Unit supporting the sensitive site exploitation did not suffer casualties because of a failure to manage risks associated with the site properly.
07	Yes/No	Enemy or adversary failed to destroy sensitive equipment, materiel, and documents or to purge computers of sensitive information before securing the site.
08	Yes/No	Commander of the unit supporting the exploitation of the sensitive site maintained situational understanding throughout the operation.
09	Yes/No	Members of the unit supporting the exploitation had access to a high fidelity common operational picture throughout the operation consistent with operations security.
10	Yes/No	Leaders of the unit supporting the exploitation of the sensitive site used the military decisionmaking process or troop leading procedures correctly to include identifying search locations, security positions, boundaries, and fire support coordination measures. They coordinated and synchronized warfighting functions.
11	Yes/No	Unit conducted operations per established rules of engagement and consideration for the nature of the sensitive site.
12	Yes/No	Unit recorded results of the search and appropriately disseminated results.
13	Yes/No	Unit supporting the exploitation of the site appropriately killed, captured, or detained enemy soldiers, adversaries, sensitive individuals, and neutrals in the site.
14	Time	Necessary to isolate the sensitive site and forces and individuals located in the site from outside physical, informational, and psychological support.
15	Time	Necessary to seize the sensitive site.
16	Time	Necessary to secure the sensitive site.
17	Time	Necessary to search the sensitive site.
18	Time	Necessary to establish liaison with and deploy technical experts to the sensitive site.
19	Percent	Of potential sensitive personnel, documents, electronic data, and materiel located in the site discovered during the search.

ART 2.3.5.4 INTELLIGENCE SUPPORT TO PERSONNEL RECOVERY

2-59. Support to personnel recovery (PR) consists of intelligence activities and capabilities focused on gathering information to recover and return U.S. personnel—whether Soldier, Army civilian, selected Department of Defense contractors, or other personnel as determined by the Secretary of Defense—who are isolated, missing, detained, or captured (IMDC) in a specific area of operation. This support also includes detailed analysis, developing detailed products, and estimates to support operations undertaken to recover IMDC personnel. (FM 3-50.1) (USACAC)

No.	Scale	Measure
01	Yes/No	Unit conducted PR-focused mission analysis.
02	Yes/No	Unit conducted PR-focused intelligence preparation of the battlefield.
03	Yes/No	Unit conducted support to PR planning, preparation, and execution.
04	Yes/No	Unit incorporated PR into intelligence, surveillance, and reconnaissance plan.

No.	Scale	Measure
05	Yes/No	Unit established PR intelligence architecture and network.
06	Yes/No	Unit established PR communications architecture and network.

ART 2.3.5.4.1 Conduct Personnel Recovery-Focused Intelligence Preparation of the Battlefield

2-60. Although the steps in the intelligence preparation of the battlefield process remain the same for all operations, analysts realize that personnel recovery operations require additional considerations. Every echelon and unit must be prepared to support personnel recovery in their area of operations and for all missions and operations executed. (FM 3-50.1) (USACAC)

No.	Scale	Measure
01	Yes/No	Unit provided weather conditions, forecasts, and updates (advisories, watches, and warnings) that provided coverage during mission period and included data pertaining to starting point, recovery site, routes to and from recovery site, and effects on the threat or local population.
02	Yes/No	Unit provided effects of weather on survivability for isolated, missing, detained, or captured personnel.
03	Yes/No	Unit queried geospatial information and services archives and available databases for information pertaining to terrain analysis of recovery site, building plans, and layout of complexes, slope, and gradient analysis of recovery site and route (to include ingress and egress routes).
04	Yes/No	If lacking sufficient geospatial information and services information, unit consulted civil affairs, psychological operations, human intelligence, and other pertinent staff or files that might have pertinent information.
05	Yes/No	Unit determined production strategy to fill geospatial data shortfalls after receiving National Geospatial-Intelligence Agency's (known as NGA) initial assessment of product and data availability and suitability.
06	Yes/No	Unit developed modified combined obstacle overlays threat, situational, and event templates.
07	Yes/No	Intelligence personnel identified potential pickup zones, landing zones, and drop zones for feasibility, defense, threats; ground and air routes for conditions, detours, hazards and obstacles; and named areas of interest and target areas of interest in vicinity of recovery site to include areas for possible suppression of enemy air defense.
08	Yes/No	Intelligence personnel identified cultural considerations of local populations in vicinity of recovery site; population safe and support status; local customs and values that impact the recovery; social and human factors that impact the recovery; political parties and factions impacts; and economic impacts.
09	Yes/No	Intelligence personnel identified known or suspected threat forces in the area (military, paramilitary, guerilla forces, insurgents, and terrorists); enemy capabilities to counter combat search and rescue (CSAR); potential enemy captivity and interrogation procedures; and special capabilities (counterintelligence, electronic measures, ground surveillance radar, night vision devices, aerial and satellite surveillance capabilities, and suspected interrogation techniques).
10	Yes/No	Intelligence personnel identified known or suspected criminal groups, gangs, and organizations that pose a risk to CSAR operations.
11	Yes/No	Unit developed an intelligence overlay of pertinent threat characteristics.
12	Yes/No	Unit coordinated with the rest of the staff to identify and post friendly units (to include multinational partners), elements, or groups in the area of operations to include coordination lines; applicable local law enforcement agencies; and political and local leaders or local populations.

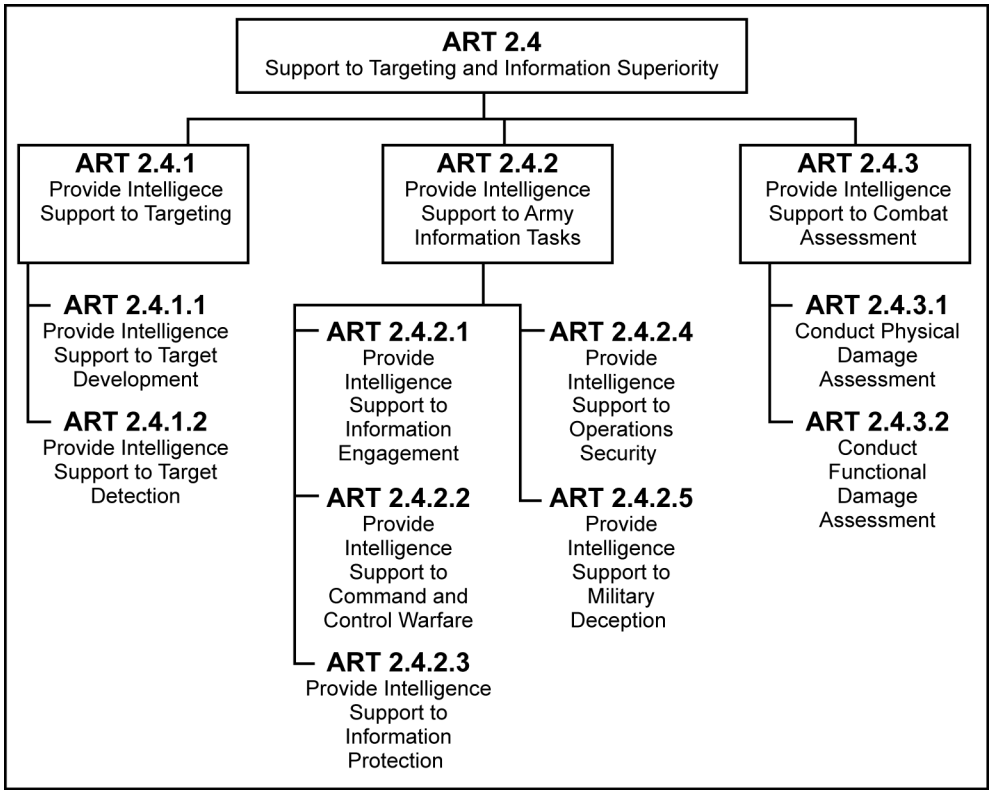
ART 2.3.5.4.2 Conduct Support to Personnel Recovery Planning, Preparation, and Execution

2-61. To accomplish the mission, the command and staff ensure resources are available to collect, analyze, and produce intelligence for the planning and execution of personnel recovery operations. The personnel

recovery (PR) intelligence support team immediately identifies the appropriate assets to best satisfy the commander's critical information requirements for PR from the available resources. To accomplish this, the team is familiar with every sensor's capabilities and limitations so they can adjust sensor taskings to ensure the optimal resource usage in real time. The intelligence, surveillance, and reconnaissance (ISR) support starts with receiving and analyzing information from the unit reporting the isolated, missing, detained, or captured (IMDC). Then the effort focuses on receiving, processing, fusing, and analyzing information originating from organic collectors and theater, joint, and national agencies and organizations. It is critical that coordination with higher headquarters is established to assist in PR operations. (FM 3-50.1) (USACAC)

No.	*Scale*	*Measure*
01	Yes/No	The command and staff ensured resources were made available to collect, analyze, and produce intelligence for planning and executing PR operations to retrieve IMDC personnel (to include contractors and Army civilians).
02	Yes/No	The staff developed a PR plan and included PR in the ISR plan.
03	Yes/No	The staff consisted of adequately trained PR personnel.
04	Yes/No	The staff tasked identified resources in accordance with the ISR annex and PR annex of the operation order.
05	Yes/No	The available assets best satisfied the requirements identified.
06	Yes/No	The available assets best satisfied the requirements tasked in the order.
07	Yes/No	The intelligence assets allocated to PR were adequate for mission accomplishment.
08	Yes/No	Unit received report of IMDC personnel.
09	Yes/No	Unit standing operating procedures IMDC report standards were met when notified of IMDC personnel.
10	Yes/No	The information on the IMDC incident was sufficient to begin PR.
11	Yes/No	Units executed their be-prepared and on-order PR tasks per the operation order.
12	Yes/No	Unit established PR intelligence and communications architecture and network.
13	Yes/No	PR intelligence and communications architecture and network were adequate.
14	Yes/No	The ISR plan required significant adjustment.
15	Yes/No	Unit completed after action review of PR plan and operation.
16	Yes/No	Unit implemented the lessons learned from the after action review into future PR planning.
17	Yes/No	The PR plan was adequate to accomplish the mission.
18	Yes/No	Higher headquarters assets were required to cover gaps in the PR plan.
19	Time	To report IMDC personnel.
20	Time	For subordinate units to reorient, move into position, or reposition to execute be-prepared and on-order PR tasks.
21	Time	To request and task assets (higher or adjacent) to reorient, move into position, or reposition to execute their PR taskings.
22	Time	To establish the PR intelligence architecture and network.
23	Time	To establish the PR communications architecture and network.
24	Time	For staff to readjust the ISR plan significantly.
25	Time	To issue the updated plan and to execute the updated plan.
26	Percent	Of significant adjustment the ISR plan required.

SECTION IV – ART 2.4: SUPPORT TO TARGETING AND INFORMATION SUPERIORITY



2-62. Intelligence support to targeting and information superiority is the task of providing the commander information and intelligence support for targeting through lethal and nonlethal actions. It includes intelligence support to the planning and execution of direct and indirect fires and the Army information tasks of information engagement, command and control warfare, information protection, OPSEC, and military deception, as well as assessing the effects of those operations. (FM 2-0) (USAICoE)

Note: This task branch supports both direct (ART 1.4) and indirect (ART 3.3) delivery of fires.

This task is also linked with ART 5.1.4.3 (Provide Combat Assessment).

No.	*Scale*	*Measure*
01	Yes/No	Targets for lethal and nonlethal action were identified, nominated, and prioritized by the entire staff.
02	Yes/No	Unit determined whether lethal, nonlethal, or a combination of lethal and nonlethal actions will achieve the best effect or the desired outcome.
03	Yes/No	Unit linked lethal and nonlethal targets to specific intelligence, surveillance, and reconnaissance (ISR) assets and included targets in the ISR plan.
04	Yes/No	Units identified ISR assets that can be retasked by the operations officer to acquire new lethal or nonlethal targets per the commander's targeting priorities.
05	Percent	Of information requirements identified for lethal and nonlethal effects.
06	Percent	Of information requirements identified for combat assessment and battle damage assessment.

No.	Scale	Measure
07	Percent	Of combat assessment and battle damage assessments that identified if targets achieved the desired effects or require reattack.
08	Percent	Of targeting databases developed, maintained, and updated.

ART 2.4.1 PROVIDE INTELLIGENCE SUPPORT TO TARGETING

2-63. The intelligence officer (supported by the entire staff) provides the fire support coordinator, information engagement officer, and electronic warfare officer, and other staff officers with information and intelligence for targeting the threat's forces and systems with direct and indirect lethal and nonlethal fires. The information and intelligence includes identification of threat capabilities and limitations. The targeting process uses the decide, detect, deliver, and assess methodology. The intelligence officer supports targeting by providing accurate, current intelligence and information to the staff and ensures the ISR plan supports the finalized targeting plan. (FM 2-0) (USAICoE)

Note: This task branch supports ART 3.2 (Detect and Locate Surface Targets) and is a byproduct of decide, detect, deliver, and assess.

No.	Scale	Measure
01	Yes/No	The intelligence officer identified threat command and control nodes, to include all aspects.
02	Yes/No	The intelligence officer identified threat communication systems, to include all aspects.
03	Yes/No	The intelligence officer identified threat computer systems, to include all aspects.
04	Yes/No	The fire support coordinator, information engagement officer, and electronic warfare officer received information and intelligence support for targeting of the threat's forces through lethal and nonlethal fires.
05	Yes/No	Risks to targeting cultural, historic sites, religious centers, medical facilities, natural resources, hazard areas (such as nuclear power plants, chemical facilities, and oil refineries) were assessed and included in target nomination criteria.
06	Time	To detect all aspects of the threat command and control nodes.
07	Time	To detect all aspects of the threat communications systems.
08	Time	To detect all aspects of the threat computer systems.
09	Time	To provide the fire support coordinator, information engagement officer, and electronic warfare officer, information and intelligence support for targeting of the threat's forces through lethal and nonlethal fires, to include updates.
10	Percent	Of threat command and control nodes vulnerable to electronic attack and electronic support.
11	Percent	Of threat computer systems vulnerable to computer network attack and computer network exploit.
12	Percent	Of threat command and control nodes disrupted and degraded.
13	Percent	Of threat command and control nodes monitored.
14	Percent	Of threat computer systems compromised.
15	Percent	Of threat computer systems monitored.

ART 2.4.1.1 PROVIDE INTELLIGENCE SUPPORT TO TARGET DEVELOPMENT

2-64. The systematic analysis of threat forces and operations to determine high-value targets (people, organizations, or military units the threat commander requires for successful completion of the mission), high-payoff targets (people, organizations, or military units whose loss to the enemy contributes significantly to the success of the friendly course of action), and systems and system components for potential attack through maneuver, fires, electronic means, or information engagement or operations. (FM 2-0) (USAICoE)

No.	Scale	Measure
01	Yes/No	Unit developed target critical components on high-value targets.
02	Yes/No	Unit refined target critical components as high-payoff targets.
03	Yes/No	Critical components passed to targeting cell in sufficient time to engage targets.
04	Yes/No	Unit identified, nominated, and prioritized targets for lethal or nonlethal action.
05	Yes/No	Staff integrated information engagement requirements into target development.
06	Yes/No	Staff identified target areas of interest associated with each lethal or nonlethal action.
07	Time	To identify, nominate, and prioritize targets for lethal or nonlethal action.
08	Time	To develop target list and perform target system analysis, critical components, vulnerability assessment, and target validation based on commander's guidance.
09	Time	To identify target areas of interest for each lethal or nonlethal action.
10	Percent	Of targeted system vulnerabilities identified correctly.
11	Number	Of correctly identified critical components in targeted systems.
12	Number	Of correctly identified targets for lethal and nonlethal action.

ART 2.4.1.2 PROVIDE INTELLIGENCE SUPPORT TO TARGET DETECTION

2-65. The intelligence officer establishes procedures for dissemination of targeting information. The targeting team develops the sensor and attack guidance matrix to determine the sensors required to detect and locate targets. The intelligence officer places these requirements into the intelligence, surveillance, and reconnaissance (ISR) synchronization tools for later incorporation into the ISR plan. (FM 2-0) (USAICoE)

No.	Scale	Measure
01	Yes/No	The intelligence officer linked targets to specific sensors for near real-time targeting and included targets in the ISR synchronization plan.
02	Yes/No	The intelligence officer included targets and sensors in the sensor and attack guidance matrix.
03	Yes/No	The intelligence officer disseminated targeting information to appropriate systems for lethal and nonlethal action.
04	Time	For sensor to pass targeting data to appropriate systems for lethal and nonlethal action.
05	Percent	Of targets linked to sensor and appropriate systems for lethal and nonlethal action.

ART 2.4.2 PROVIDE INTELLIGENCE SUPPORT TO ARMY INFORMATION TASKS

2-66. Intelligence support to information tasks is the task of providing the commander information and intelligence support for targeting through nonlethal actions. It includes intelligence support to the planning, execution of the Army information tasks (information engagement, command and control warfare, information protection, operations security, and military deception), as well as assessing the effects of those operations. Key activities reflected in this task include communications, planning, synchronization, and integration of intelligence into operation plans and orders. (FM 3-0) (USACAC)

Note: This task branch only addresses those intelligence tasks that support the conduct of Army information tasks. The actual conduct of information engagement, information protection operations, and activities related to command and control warfare are tasks addressed elsewhere in the FM 7-15:

- ART 3.4 (Integrate Command and Control Warfare) addresses the conduct of electronic command and control warfare operations.
- ART 6.3 (Conduct Information Protection) addresses the conduct of passive measures that protect information and systems.

- ART 6.11.3.1 (Conduct Counterintelligence Operations) addresses the conduct of that particular task which also relates to ART 6.3 (Conduct Information Protection).
- ART 5.3.1 (Integrate Information Engagement Capabilities) is the other activity related to Army information tasks.

No.	Scale	Measure
01	Yes/No	Intelligence support to targeting database maintained.
02	Yes/No	Information operations (IO) target identified, prioritized and nominated.
03	Yes/No	Intelligence support identified for each element of IO involved in the operation and integrated into the intelligence, surveillance, and reconnaissance plan.
04	Yes/No	Battle damage assessment performed on IO targets and target systems.
05	Yes/No	Combat assessment performed on IO targets.
06	Time	To determine support required for IO.
07	Time	To determine specific information requirements for IO.
08	Time	To determine the effects on the IO targets engaged.
09	Time	To provide combat assessments in support of IO.
10	Percent	Of IO requirements answered.

ART 2.4.2.1 PROVIDE INTELLIGENCE SUPPORT TO INFORMATION ENGAGEMENT

2-67. Military intelligence organizations operating outside U.S. territories support activities related to information engagement under some circumstances. (FM 2-0) (USAICoE)

No.	Scale	Measure
01	Yes/No	Unit identified intelligence support required for public affairs through intelligence preparation of the battlefield.
02	Yes/No	Unit provided intelligence and information to identify pertinent civil considerations that affect information engagement.
03	Yes/No	Unit provided intelligence support to identify populace perceptions, sentiments, attitudes, mores, allegiances, alliances, and behaviors.
04	Yes/No	Unit provided intelligence support to identify nongovernmental and international organizations in the operational environment.
05	Yes/No	Unit provided identification support of resources and capabilities of nongovernmental and international organizations in the operational environment.
06	Yes/No	Unit identified all relevant government agencies, organizations, or departments that affect public affairs activities.
07	Yes/No	Unit provided intelligence support to identify adversary misinformation, disinformation, and propaganda capabilities.
08	Yes/No	Unit provided intelligence support to identify the location, biases, and agenda of national media representatives in the operational environment.
09	Yes/No	Unit provided intelligence support to identify the location, biases, and agenda of international media representatives in the operational environment.
10	Yes/No	Unit provided intelligence support to identify trends reflected by the national and international media.
11	Yes/No	Unit provided intelligence and information to public affairs per all applicable regulations, policies, and laws.

ART 2.4.2.1.1 Provide Intelligence Support to Public Affairs

2-68. This task entails military intelligence organizations collecting and providing information and intelligence products concerning civil considerations in the area of operations to support public affairs activities. (FM 2-0) (USAICoE)

No.	Scale	Measure
01	Yes/No	Intelligence support required for public affairs identified through intelligence preparation of the battlefield.
02	Yes/No	Unit provided intelligence information to identify pertinent civil considerations that affect public affairs activities and operations.
03	Yes/No	Unit provided intelligence support to identify populace perceptions, sentiments, attitudes, mores, allegiances, alliances, and behaviors.
04	Yes/No	Unit provided intelligence support to identify nongovernmental and international organizations in the operational environment.
05	Yes/No	Unit identified all relevant government agencies, organizations, or departments that affect public affairs activities and operations.
06	Yes/No	Unit provided intelligence support to identify trends reflected by the national and international media.
07	Yes/No	Unit provided intelligence support to identify the location, biases, and agenda of national media representatives in the operational environment.
08	Yes/No	Unit provided intelligence support to identify the location, biases, and agenda of international media representatives in the operational environment.
09	Yes/No	Unit provided intelligence support to identify adversary misinformation, disinformation, and propaganda capabilities.
10	Yes/No	Unit provided intelligence and information to public affairs per all applicable regulations, policies, and laws.
11	Time	To identify pertinent civil considerations which affect public affairs activities and operations.
12	Time	To identify populace perceptions, sentiments, attitudes, mores, allegiances, alliances, and behaviors.
13	Time	To identify nongovernmental and international organizations in the operational environment.
14	Time	To identify all relevant government agencies, organizations, or departments that affect public affairs activities and operations.
15	Time	To identify trends reflected by the national and international media.
16	Time	To identify the location, biases, and agenda of national media representatives in the operational environment.
17	Time	To identify the location, biases, and agenda of international media representatives in the operational environment.
18	Time	To identify adversary or enemy misinformation, disinformation, and propaganda capabilities.
19	Percent	Of accurate information and intelligence provided to public affairs for civil considerations that affect public affairs activities and operations.

ART 2.4.2.1.2 Provide Intelligence Support to Psychological Operations

2-69. Psychological operations require information and intelligence to support analysis of foreign target audiences and their environment to include the following factors: political, military, economic, social, social, information, infrastructure, physical environment and time. Continuous and timely intelligence is required to assess target audience behavioral trends. Information and intelligence focus on target audience motivation and behavior; indicators of success or lack of success (measure of effectiveness); and the target audience's reaction to friendly, hostile, and neutral force actions. (FM 2-0) (USAICoE)

No.	Scale	Measure
01	Yes/No	Unit identified intelligence support required for psychological operations through intelligence preparation of the battlefield and support to targeting.
02	Yes/No	Unit responded to psychological operations specific information requirements concerning the civil considerations.
03	Yes/No	Unit completed combat assessment on psychological operations targets.
04	Time	To determine the effects on the psychological operations targets engaged.

No.	Scale	Measure
05	Time	To provide combat assessments in support of psychological operations.
06	Percent	Of psychological operations information requests to which unit responded.

ART 2.4.2.2 PROVIDE INTELLIGENCE SUPPORT TO COMMAND AND CONTROL WARFARE

2-70. Military intelligence organizations provide information to identify threat decisionmaking and command and control nodes, processes, and means in order of criticality. Intelligence also helps identify threat systems, activities, and procedures that may be vulnerable to command and control warfare. Additionally, intelligence plays a key role in evaluating and assessing the effectiveness of command and control warfare. (FM 2-0 (USAICoE)

Note: This task supports electronic attack which employs jamming, electromagnetic energy, or directed energy against personnel, facilities, or equipment. This task identifies critical threat information systems and command and control nodes.

No.	Scale	Measure
01	Yes/No	Unit identified threat command and control nodes.
02	Yes/No	Unit identified threat communications systems.
03	Yes/No	Unit identified threat computer systems.
04	Yes/No	Intelligence support required for electronic attack identified through intelligence preparation of the battlefield and support to targeting.
05	Yes/No	Unit identified the threat's assets, processes, patterns, and means vulnerable to electronic attack.
06	Yes/No	Unit provided intelligence support to locate targets for electronic attack.
07	Yes/No	Unit provided intelligence support to determine if desired effects were achieved.
08	Yes/No	Unit provided information regarding target capabilities and vulnerabilities.
09	Yes/No	Unit provided information regarding which enemy systems are available against which to perform electronic attack.
10	Yes/No	Unit completed combat assessment for electronic attack.
11	Time	To determine support required for electronic attack.
12	Time	To determine specific information requirements for electronic attack.
13	Time	To provide combat assessments in support of electronic attack.
14	Percent	Of threat command and control nodes vulnerable to electronic attack.
15	Percent	Of threat command and control nodes vulnerable to electronic exploitation.
16	Percent	Of threat computer systems vulnerable to computer network attack.
17	Percent	Of threat command and control nodes disrupted and degraded.
18	Percent	Of threat computer systems compromised.
19	Percent	Of personnel, facilities, or equipment degraded, denied, disrupted, or destroyed by electronic attack.

ART 2.4.2.3 PROVIDE INTELLIGENCE SUPPORT TO INFORMATION PROTECTION

2-71. The military intelligence organizations provide information to identify threat command and control warfare capabilities and activities and tactics, techniques, and procedures. Intelligence provides information relating to computer network defense, physical security, operations security, counterdeception, and counterpropaganda. (FM 2-0) (USAICoE)

No.	Scale	Measure
01	Yes/No	Intelligence support required for information protection identified through intelligence preparation of the battlefield and support to targeting.
02	Yes/No	Unit identified threat offensive information capabilities.
03	Yes/No	Unit identified threat offensive information operations (IO) tactics, techniques, and procedures.
04	Yes/No	Unit identified friendly assets and forces that the threat could exploited.
05	Yes/No	Unit completed combat assessment on threat offensive IO.
06	Time	That threat offensive IO disrupts, degrades, or exploits friendly information systems.
07	Percent	Of known threat sensor coverage in area of operations.
08	Percent	Of attempted threat penetration of friendly information systems and facilities that were successfully defeated.
09	Percent	Of imitative electronic deception attempted and successful against our forces.
10	Percent	Of threat IO capabilities not covered by operations security measures.
11	Percent	Of procedures for information protection changed or modified based on the results of combat assessment.
12	Number	Of threat offensive IO attempts that disrupt, degrade, or exploit friendly information systems and facilities.
13	Number	Of imitative electronic deception operations against our forces.

ART 2.4.2.4 PROVIDE INTELLIGENCE SUPPORT TO OPERATIONS SECURITY

2-72. This task identifies capabilities and limitations of the threat's intelligence system including adversary intelligence objectives and means, procedures, and facilities to collect, process, and analyze information. This task supports the identification of indicators that adversary intelligence capabilities and systems might detect that could be interpreted or pieced together to obtain essential elements of friendly information in time to use against friendly forces. (FM 2-0) (USAICoE)

No.	Scale	Measure
01	Yes/No	Intelligence support required for operations security identified through intelligence preparation of the battlefield.
02	Yes/No	Unit identified capabilities and limitations of adversary, threat intelligence, and security services.
03	Yes/No	Unit identified operations security compromises.
04	Time	To input the information operations annex of the operation order.
05	Time	To identify potential compromises of essential elements of friendly information in area of operations (AO).
06	Number	Of adversary capabilities in the AO identified.
07	Number	Of successful adversary attempts to obtain information concerning friendly information systems.
08	Number	Of encrypted communications in AO.
09	Number	Of operations security measures selected tied to vulnerability analysis.
10	Number	Of operations security vulnerabilities tied to specific adversary capabilities by planners.

ART 2.4.2.5 PROVIDE INTELLIGENCE SUPPORT TO MILITARY DECEPTION

2-73. This task identifies capabilities and limitations of the threat's intelligence collection capabilities, systems, and means and identifies threat biases and perceptions. (FM 2-0) (USAICoE)

No.	Scale	Measure
01	Yes/No	Unit identified profiles of key threat leaders.
02	Yes/No	Unit outlined the threat decisionmaking processes, patterns, and biases.

No.	Scale	Measure
03	Yes/No	Unit identified the threat's decisionmaking dissemination processes, patterns, and means.
04	Yes/No	Unit identified the threat perceptions of the military situation in the area of operations.
05	Yes/No	Unit identified capabilities and limitations of threat intelligence and security services.
06	Yes/No	Unit completed combat assessment for deception operations.
07	Time	To determine support required for deception operations.
08	Time	To determine specific information requirements for deception.
09	Time	To provide combat assessments in support of deception.
10	Percent	Of threat forces and targets who were deceived.

ART 2.4.3 PROVIDE INTELLIGENCE SUPPORT TO COMBAT ASSESSMENT

2-74. Intelligence supports the assess activity of the operations process and targeting processes. The commander uses combat assessment to determine if targeting actions have met the attack guidance and if reattack is necessary to perform essential fires tasks and achieve the commander's intent for fires. The staff determines how combat assessment relates to specific targets by completing battle damage, physical damage, functional damage, and target system assessments. (FM 2-0) (USAICoE)

Note: This task branch supports ART 5.1.4 (Assess Tactical Situations and Operations), ART 5.1.4.3 (Provide Combat Assessment), and ART 5.1.4.3.1 (Perform Battle Damage Assessment). It is also associated with decide, detect, deliver, and assess.

No.	Scale	Measure
01	Yes/No	Unit identified intelligence, surveillance, and reconnaissance assets that can acquire information on target effects.
02	Yes/No	Unit provided an initial assessment of attacks.
03	Yes/No	Unit provided a full assessment of attacks.
04	Time	To identify and submit information requirements for lethal and nonlethal effects.
05	Time	To identify and submit information requirements for combat assessment and battle damage assessment.
06	Time	To perform combat assessment to identify if targets achieved the desired effects or require reattack.
07	Time	To make initial assessment of attacks after engagement.
08	Time	To provide initial assessment of attack effects to force commander.
09	Time	To complete full assessment of attack effects after engagement.
10	Time	To provide full assessment of attacks to force commander.
11	Time	To provide reattack recommendations.
12	Percent	Of high-payoff targets correctly assessed to meet attack guidance.

ART 2.4.3.1 CONDUCT PHYSICAL DAMAGE ASSESSMENT

2-75. Conduct physical damage assessment is a staff task that estimates the extent of physical damage to a target based on observed or interpreted damage. It is a post attack target analysis that is a coordinated effort among all units and the entire staff. (FM 2-0) (USAICoE)

No.	Scale	Measure
01	Yes/No	Unit identified intelligence, surveillance, and reconnaissance assets that can acquire information for physical damage assessment.
02	Yes/No	Unit provided an initial assessment of physical damage.
03	Yes/No	Unit provided a full assessment of attacks.

No.	Scale	Measure
04	Yes/No	Unit provided reattack recommendations.
05	Time	To identify and submit information requirements for physical damage assessment.
06	Time	To make initial assessment of physical damage after engagement.
07	Time	To provide initial assessment of physical damage to force commander.
08	Time	To complete full assessment of physical damage.
09	Time	To provide full assessment of attacks to force commander.
10	Percent	Of physical damage achieved within the commander's intent for fires.
11	Percent	Of targets correctly assessed for the commander's intent for fires.
12	Percent	Of targets unnecessarily reattacked.

ART 2.4.3.2 CONDUCT FUNCTIONAL DAMAGE ASSESSMENT

2-76. The staff conducts the functional damage assessment for the threat's remaining functional or operational capabilities. The assessment focuses on measurable effects. It estimates the threat's ability to reorganize or find alternative means to continue operations. The targeting working group and staff integrate analysis with external sources to determine if the commander's intent for fires has been met. (FM 2-0) (USAICoE)

No.	Scale	Measure
01	Yes/No	Unit identified intelligence, surveillance, and reconnaissance assets that can acquire information for functional damage assessment.
02	Yes/No	Unit provided an initial assessment of functional damage.
03	Yes/No	Unit provided a full assessment of attacks.
04	Yes/No	Unit provided reattack recommendation.
05	Time	To identify and submit information requirements for functional damage assessment.
06	Time	To make initial assessment of functional damage after engagement.
07	Time	To provide initial assessment of functional damage to force commander.
08	Time	To complete full assessment of functional damage.
09	Time	To provide full assessment of attacks to force commander.
10	Percent	Of functional damage achieved within the commander's intent for fires.
11	Percent	Of targets correctly assessed for the commander's intent for fires.
12	Percent	Of targets unnecessarily reattacked.