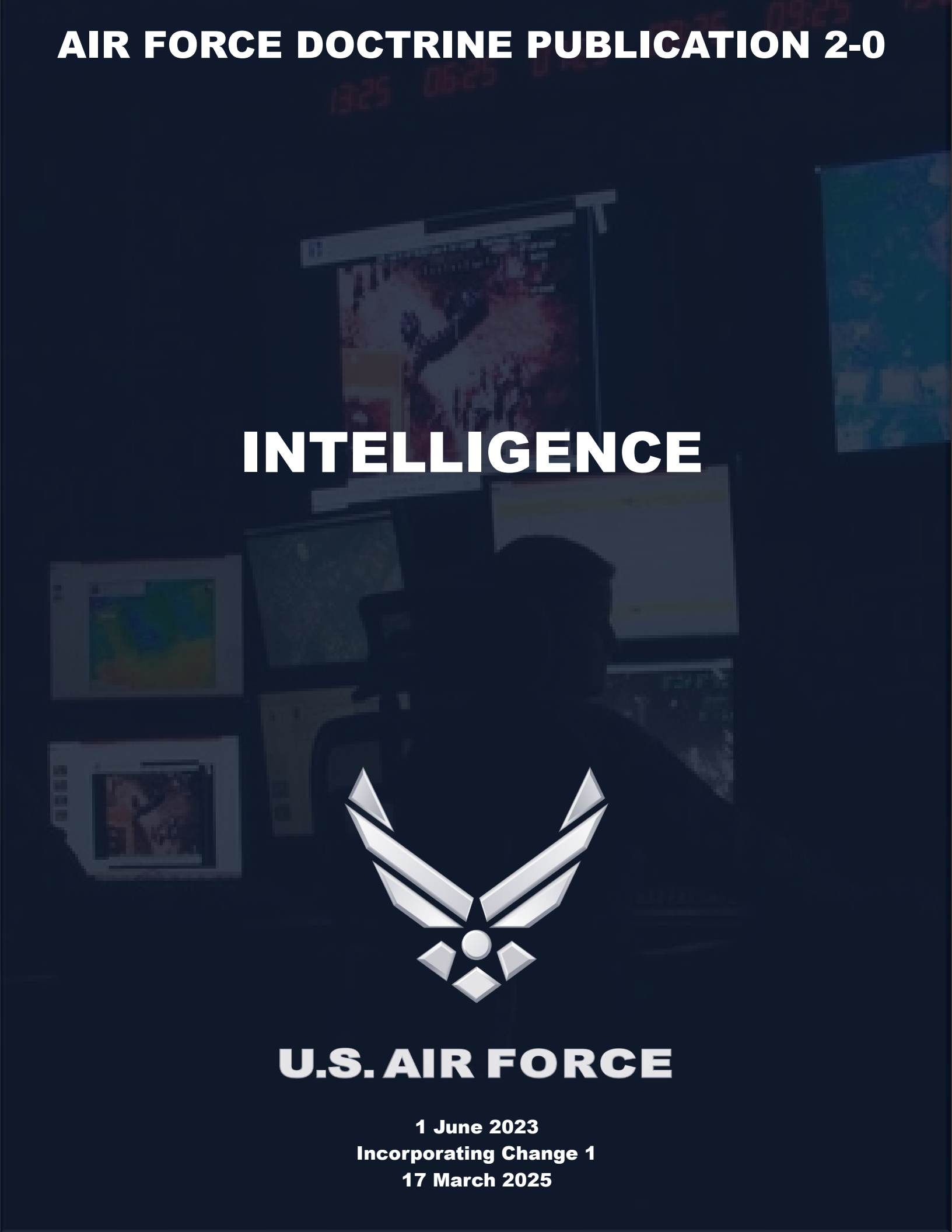
AIR FORCE DOCTRINE PUBLICATION 2-0



INTELLIGENCE

U.S. AIR FORCE

1 June 2023
Incorporating Change 1
17 March 2025

Air Force Doctrine Publication 2-0, *Intelligence*

Table of Contents

"The Air Force organizes, trains, and equips forces to be an air component to a joint force commander (JFC). As part of the joint force's air component, our forces must be prepared to accomplish JFC objectives**.** The air component commander's administrative authorities are derived from Title 10, U.S. Code, and exercised as the commander, Air Force forces (COMAFFOR). The air component commander's operational authorities are delegated from the JFC and exercised as both the COMAFFOR, over Air Force forces, and as the functional joint force air component commander (JFACC), over joint air forces made available for tasking. Thus, the air component commander leads Air Force forces as the COMAFFOR and the JFC's joint air operations as the JFACC. This duality of authorities is expressed in the axiom: Airmen work for Airmen and the senior Airman works for the JFC."

-- Air Force Doctrine Publication (AFDP) 1, *The Air Force*

Since the COMAFFOR and JFACC are nearly always the same individual, this AFDP will use the term "air component commander" when referring to duties or functions that could be carried out by either or both, unless explicit use of the term "COMAFFOR" or "JFACC" is necessary for clarity.

CHAPTER 1: INTELLIGENCE OPERATIONS

Intelligence operations illuminate the strategic, operational, and tactical environment, clarify adversary intentions, and are critical to commander decision-making across the competition continuum. Intelligence includes the organizations, capabilities and processes used to task, collect, process, analyze, and exploit single-source intelligence. With an enduring focus on satisfying joint force commander (JFC) intelligence requirements, intelligence operations are conducted in, from, and through all domains across the competition continuum.

Intelligence operations encompass all-domain intelligence collection through the full spectrum of sensor capabilities and the integrated processing, exploitation, analysis, and production activities at the unit level, air operations centers (AOCs), distributed ground stations (DGSs), and national production centers. These operations produce and disseminate intelligence to tactical, operational, and strategic users through the joint intelligence process: planning and direction; collection, processing, and exploitation; analysis and production; dissemination; and evaluation and feedback (PCPADE). Importantly, evaluation and feedback are continuous and facilitated throughout the process by collaborative dialogue with all stakeholders.

Directly supporting current and future intelligence operations, intelligence, surveillance, and reconnaissance (ISR) is an activity that synchronizes and integrates the planning and operation of sensors; assets; processing, exploitation, and dissemination (PED) systems; and analytic systems or capabilities. ISR operations comprise the primary activities that feed data and information into the joint intelligence process. As a result, ISR is often the first capability a combatant commander (CCDR) requests before commencing operations. Moreover, ISR operations often persist after other operations have ceased. They are continuous, in high demand, and can act as a demonstration of the United States' (US) global power.

Although intelligence is produced by various specialties across the Department of Defense (DOD) and the intelligence community, it should be treated as a globally integrated whole. The goal for intelligence is to enable decision advantage by providing a comprehensive and cohesive awareness of the operating environment. Doing so requires an integrated approach; one that combines data and intelligence from joint, departmental, national, and multinational capabilities. Towards this aim, United States Air Force (USAF) intelligence forces integrate, fuse, tailor, and analyze collected information and data to deliver timely intelligence, when and where needed, anywhere around the globe.

Intelligence is the linchpin of an effects-based approach to operations (EBAO). Intelligence operations are domain, sensor, and Service agnostic. The focus is on meeting information requirements and providing actionable intelligence to commanders at the right time and place. The integration and synchronization of assets, people, processes, and information across all domains is critical to achieve decision advantage.

INTELLIGENCE VS. ISR

The terms intelligence and ISR are often used interchangeably. In many contexts their differences are subtle enough. However, with respect to this doctrine there are important distinctions worth noting and it becomes increasingly important to differentiate between the two.

Joint Publication 2-0, *Joint Intelligence*, provides the following definitions:

- **Intelligence.** 1. **The product** resulting from the collection, processing, integration, evaluation, analysis, and interpretation of available information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations. 2. **The activities** that result in the product. 3. **The organizations** conducting such activities.
- **ISR.** 1. An integrated operations and intelligence **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. 2. **The organizations** or assets conducting such activities.

Both terms refer to activities and the organizations that conduct them. To discern between the two, it is important to identify their purpose or aim. ISR activities produce information and data. Through the joint intelligence process, information and data is then used to produce intelligence. From this perspective, ISR is a subordinate intelligence activity conducted to gather information and data necessary to meet intelligence requirements. With this understanding, uses of each term in this publication are intended to be as deliberate and accurate as possible.

EXCELLENCE IN INTELLIGENCE

Intelligence should be **anticipatory, timely, accurate, usable, complete, relevant, objective, and discoverable.**[1]

- Intelligence should **anticipate** the air component's intelligence needs for current and future operations and be involved in air operations planning as early as possible.
- Intelligence should be **discoverable**, **objective**, and presented to commanders in a **timely** manner to facilitate decision advantage.
- Intelligence should convey the **accuracy**, **quality**, and confidence regarding the information and its source.
- Intelligence should be **usable** and **complete** to meet the air component's unique command and control requirements against the enemy's most likely and most dangerous courses of action.

[1] For additional information on excellence in intelligence, see Joint Publication (JP) 2-0, *Joint Intelligence.*

- ✪ Intelligence should remain **relevant** to air operations by staying mindful of indicators that could hamper or present challenges for the air component.

KEY PRINCIPLES OF USAF INTELLIGENCE OPERATIONS

Intelligence analysts retain a theater-wide perspective of threats. They prioritize based on commander's intent and synchronize intelligence with plans and operations. Analysts assess and anticipate risk posed by threats, collaborate to leverage analytic expertise, and exploit all sources of information and intelligence through fusion and application of analytic tradecraft.

USAF intelligence analysts follow the principles of joint intelligence.[2] Additionally, **integration**, **survivability**, **sustainability**, **deployability**, and **network-centricity** are key principles enabling theater-wide air component intelligence operations. Intelligence personnel should be fully aware of mission goals and objectives and be integrated at all levels.

Intelligence resources, activities, communications, capabilities, and capacity should be **survivable** to ensure availability when needed. Essential components of survivability include redundancy of critical intelligence, protection against asymmetric adversary threats (e.g., ISR mission assurance), and information assurance.

Intelligence operations should be **sustainable**. An ISR system's ability to maintain the necessary level and duration of operations depends on ready forces and resources in sufficient quantities to support stated requirements.

Intelligence capabilities are **deployable** or may be provided through reachback to support expeditionary operations. Deployable supporting assets can be rugged, small, and lightweight. They should be easy to transport, set up, and capable of immediate connectivity and interoperability. Extensive reachback support, Distributed Common Ground System (DCGS), and national intelligence centers enhance the intelligence process, as do overall analytical capabilities within the intelligence enterprise in support of global missions from the continental US and overseas locations.

Network-centricity enables intelligence personnel to provide tailored, actionable intelligence that increases situational awareness and fosters increased flexibility and responsiveness. Network-centric collaborative environments enable efficient use of finite intelligence resources and facilitate data flow among networks at various classification and releasability levels. This approach ensures ISR sensor data is posted to compatible, joint intelligence information repositories for broader use. It also provides better connections among foreign partner resources via virtual organizations. In addition, virtual collaborative environments allow intelligence personnel from numerous agencies to horizontally align as a team, focus analytic efforts, and respond to intelligence requirements with answers or recommended courses of action enabling decision advantage.

[2] For additional information on the principles of joint intelligence, see JP 2-0.

AIR COMPONENT INTELLIGENCE SUPPORT

Air component intelligence support enables decision advantage for joint and coalition forces through three integrated capabilities: battlespace characterization, collection operations, and targeting. These capabilities are delivered to the CCMD or joint task force (JTF) through divisions of the AOC.

BATTLESPACE CHARACTERIZATION

The purpose of battlespace characterization is to understand and predict an adversary by examining their capabilities, tactics, dispositions, center(s) of gravity, and courses of action within the context of the operating environment. It is critical for providing indications and warnings, identifying potential vulnerabilities to forces, and identifying opportunities to achieve objectives. The aim of battlespace characterization is to identify what is and is not known by continuously updating and validating assessments. Information gained through battlespace characterization is a valuable foundation to inform targeting.

COLLECTION OPERATIONS

Collection operations acquire raw data and information about relevant aspects of the operational environment and provide that information to intelligence processing and exploitation elements. Collection involves tasking and synchronizing ISR sensors, platforms, and exploitation resources to characterize the operational environment, adversary activities, and infrastructure, and to target (i.e., find, fix, track, target) entities in the battlespace. The aim is to test beliefs, confirm knowledge, and discover intelligence gaps to enhance decision advantage. Collection operations are typically driven by battlespace characterization or targeting requirements.

TARGETING

Targeting is the process of selecting and prioritizing targets and matching the appropriate response to them, considering operational requirements and capabilities.[3] Targeting requires a continuous, analytic process to identify, develop, and affect targets to meet commander objectives. Intelligence, including ISR activities to find, fix, track, and target entities, is a critical component of each of the six targeting process steps. Targeting is interdisciplinary and requires the expertise of personnel from many functional disciplines.

Examples of Functional Disciplines that Support Targeting

- Strategists and planners bring knowledge of the context and integrated plans.
- Personnel involved in combat operations bring recent experience.
- Intelligence personnel provide analysis of adversary strengths and vulnerabilities and targeting expertise.
- Judge advocates apply the law of war and interpret rules of engagement for mission planning and weapons delivery.

[3] For additional information, see JP 3-60, *Joint Targeting*.

INTELLIGENCE ROLES IN OPERATIONS

OPERATIONAL UNIT-LEVEL INTELLIGENCE.

In support of major combat operations, individual unit-level intelligence teams are organized collectively to form the contingency intelligence network (CIN).[4] The core wing intelligence teams are the combat intelligence cell (CIC), mission planning cell (MPC), and squadron intelligence. The CIN funnels all intelligence into and out of a particular wing or organization to support three main functions: mission planning, mission execution, and mission debriefing and reporting.

At the operational level, the CIC interacts with an AOC ISR division's (ISRD's) unit support function to gather current intelligence, threat data, and request for information (RFI) responses. They disseminate this information throughout the wing and down to operational squadrons. The MPC provides analysis of possible enemy courses of action, provides support to targeting, and delivers timely updates to operational mission planners. Squadron intelligence personnel support specific airframes and are responsible for communicating relevant intelligence directly to aircrew. The CIN, through the CIC, MPC, and squadron intelligence, keeps the commander and operations crews informed of intelligence that can affect mission execution. Support may include intelligence databases, current threat briefings and training, and assistance with mission planning.

USAF SPECIAL OPERATIONS

USAF special operations are intelligence-intensive and, in some cases, require detailed and tailored intelligence support. Special operations forces (SOF) support tends to rely on organic ISR assets, be less centralized, and focus on tactical intelligence. Intelligence personnel produce detailed, specialized products tailored to the mission, customer, and pace of operation. The sensitivity of SOF missions may constrain the release of post-mission reports. Commanders should report sensitive mission data through special access or routine intelligence channels accordingly.

HOMELAND OPERATIONS

When lawful and authorized to do so, USAF intelligence forces may be tasked to conduct ISR or incident awareness and assessment (IAA) within the homeland. Though similar to ISR, IAA operations are conducted during defense support of civil authorities (DSCA) activities, providing timely and usable information to commanders and local, tribal, state, and federal leaders to save lives, reduce human suffering, and protect property. Though ISR activities may be conducted within the US for homeland defense, IAA is only conducted within the US for DSCA.

Importantly, the laws governing DOD operations in the homeland are different than those that govern overseas operations. These laws place specific restrictions and limitations on the employment or use of military intelligence in the homeland.[5]

---

[4] For additional information, see Air Force Tactics, Techniques, and Procedures (AFTTP) 3-4.14, *Contingency Intelligence Network*.
[5] For additional information, see Air Force Doctrine Publication (AFDP) 3-27, *Homeland Operations*.

NUCLEAR OPERATIONS

Nuclear operations require focused and detailed intelligence that can survive in pre- and post-strike environments. Intelligence provides commanders with information needed to make timely decisions and enables civilian leaders to send clear messages and signals to deter adversaries and assure allies.[6]

CYBERSPACE OPERATIONS

Cyberspace operations that support air operations are usually provided to the air component through reachback and are broken down into three subsets: offensive (OCO), defensive (DCO), and Department of Defense Information Network (DODIN) operations. Intelligence support to each of these subsets is technologically focused and requires significant technical understanding of the domain. Cyberspace intelligence analysts should be integrated as closely as possible with cyberspace personnel.

Intelligence for OCO identifies access vectors to gain entry into adversarial target networks, detail target network characteristics, and identify network vulnerabilities for further attack vectors. Intelligence analysts supporting DCO and DODIN operations consider the perspective of potential adversaries that may attack air component networks to understand threats to those systems, whether from state or non-state actors.[7]

IRREGULAR WARFARE

USAF intelligence provides significant capability in irregular warfare. Irregular warfare focused intelligence analysts assess indicators such as the level of cooperation with local nationals and the capability to train partner forces to conduct independent and multinational operations. Intelligence forces use information from various sources, focusing on those in the best position to provide or collect information to fill intelligence gaps. Care is given to validate the credibility of sources to overcome adversary denial, deception, and disinformation. Intelligence shared to support irregular warfare should include authorized partners (e.g., local law enforcement, allies or coalition partners, or non-governmental organizations) participating in the operation that have a need to know.

FORCE PROTECTION

Intelligence provides vital support and capabilities to force protection functions and activities to defeat threats to airfields and air bases and prevent mission degradation. If tasked to defend assets and personnel at air component installations, the air component commander should consider designating organic ISR assets to support the Air Force Office of Special Investigations (AFOSI) counterintelligence (CI) activities.

Force protection forces rely on the unique capabilities of various sensors to develop a comprehensive understanding of the operational environment and enhance their ability to identify and track potential threats. Intelligence support to force protection operations should identify threats and focus on ways to mitigate or eliminate them. Achievement of

[6] For additional information, see AFDP 3-72, *Nuclear Operations.*
[7] For additional information, see AFDP 3-12, *Cyberspace Operations.*

JFC and air component commander force protection objectives can be aided by the proper combination of complementary ISR and force protection activities and capabilities.[8]

[8] For additional information, see AFDP 3-10, *Force Protection.*

CHAPTER 2: COMMAND AND CONTROL, FORCE PRESENTATION, AND ORGANIZATION

COMMAND AND STAFF RESPONSIBILITIES

Command relationships delineate the degree of authority commanders have over forces. Understanding these authorities and how they fit into the planning and direction portion of the PCPADE process is critical for intelligence operations.

DEPARTMENT OF DEFENSE

The air component's allocated ISR capabilities are coordinated globally. The DOD develops the annual global theater ISR allocation plan and provides ISR sourcing recommendations for emergent CCDR requests and national intelligence requirements. PED capacity is then aligned with DOD ISR allocation. Gaps in capability and shortfalls in capacity should be identified. Finally, the DOD, CCDRs, air components, and Services develop strategies and plans to integrate and synchronize the employment of national, DOD, and international partner capabilities.

COMBATANT COMMANDER

CCDRs employ assigned and attached intelligence forces to achieve national and theater objectives. When additional forces are required, CCDRs submit a request for forces (RFF) through the global force management process. When authorized, CCMDs may also coordinate to enable the cooperative use of assets not regularly assigned to them to improve coverage. Based on guidance and direction from the CCDR, intelligence (J2) and operations (J3) staffs develop an overall theater collection strategy and posture for executing intelligence operations.

The CCDR may delegate operational control (OPCON) or tactical control (TACON) over theater ISR assets to appropriate subordinate commanders. However, the CCDR retains the authority to validate and prioritize requirements for collection by theater ISR assets. At the theater level, CCDRs exercise collection management authority (CMA) for collection operations within their area of responsibility.[9]

Collection Management Authority. CMA is the authority to establish, prioritize, and validate theater collection requirements, establish sensor tasking guidance, and develop theater-wide collection policies. Commanders exercising OPCON over intelligence forces may assume CMA of tasked ISR assets as part of the delegation of authority. The theater J2 usually retains CMA to validate, modify, or non-concur theater intelligence requirements through the CCDR's joint intelligence operations center.

CMA usually includes the authority to task geospatial-intelligence sensors and lower-echelon signals intelligence (SIGINT) collection systems with more localized collection capabilities. The National Security Agency (NSA) retains CMA over strategic-capable SIGINT ISR systems. In addition, CCDRs may request, and subsequently receive,

[9] For additional information on collection management, see JP 2-0.

temporary SIGINT operational tasking authority (SOTA) over theater-wide capable platforms and sensors. The delegation of SOTA to a CCDR and subsequent delegation of this authority to the JFC ensures the theater can prioritize requirements and focus SIGINT collection where needed to carry out assigned missions. Collection management includes two complementary functions: collection requirements management (CRM) and collection operations management (COM).

- **Collection Requirements Management.** CRM is the authoritative development and control of collection, processing, exploitation, and information reporting requirements. It is focused on the customer's requirements, is all-source oriented, and indicates necessary information for collection. This process typically results in the requests generated to CMAs at higher, lower, or lateral echelons to accomplish the collection mission or by tasking requirements to units within the command. CRM and validation of collection requirement requests often reside at the CCDR level or may be delegated to a subordinate JFC.

- **Collection Operations Management.** COM is the authoritative direction, scheduling, and control of specific collection operations and associated processing, exploitation, and information reporting resources. COM is often delegated to an echelon below the JFC (usually the air component commander) when that echelon has the required expertise in daily collection operations for specific ISR assets. COM delegation differs during contingency and steady-state operations. During steady-state, COM for USAF ISR assets is typically delegated to the Service in accordance with CCMD priorities. During wartime, if COM is delegated, it is usually delegated to the air component commander.

Collected data may be provided to multiple theaters simultaneously. The Under Secretary of Defense for Intelligence and Security has delegated CMA to the Defense Intelligence Agency (DIA) and designated DIA as the defense intelligence enterprise manager for collection management.

JOINT FORCE COMMANDER

The JFC establishes priorities for intelligence operations that align with national and theater objectives and ensures theater planning efforts support the fulfillment of crisis intelligence requirements. High priority, time-sensitive requirements are identified and pre-validated by the JFC for the air component commander to consider for dynamic retasking during the execution of intelligence operations. When theater requirements exceed the capacity of assigned and attached forces, the JFC or air component commander may submit requests for forces through the CCMD for additional ISR capabilities (personnel, platforms, etc.). Taskings involving ISR assets supporting more than one JFC are coordinated and deconflicted by a common superior commander.

The JFC’s staff is responsible for developing a collection strategy and execution posture for these ISR missions and coordinating with national agencies. The JFC J2 reviews, validates, and prioritizes all outstanding intelligence requirements, whether originating with the JFC J2 staff or subordinate components. In conjunction with component staffs, the JFC's staff is responsible for developing a shared production architecture that

leverages reachback, distributed, and federated partners for intelligence exploitation and analysis. This shared production architecture also leverages the support of organic capabilities at the component and JTF level, the Services, other CCDRs, foreign partners, and national agencies. This helps maximize coverage of intelligence requirements.

With any command relationship pertaining to intelligence forces, care should be taken to understand and align the authorities of Title 10, U.S.C., *Armed Forces,* and Title 50, U.S.C., *War and National Defense* to avoid potential conflicts.

AIR COMPONENT COMMANDER

The JFC normally delegates OPCON of assigned or attached airborne ISR assets to the air component commander. The air component commander is typically the supported commander for theater ISR and is often delegated responsibility for COM. The JFC often retains CRM authority, but as the supported commander for theater ISR, the air component commander can leverage the AOC to integrate CRM and COM.

Collection managers communicate air component commander taskings through scheduling messages and a prioritized list of collection objectives. Specific collection objectives are then tasked in the reconnaissance, surveillance, and target acquisition (RSTA) annex to the air tasking order (ATO). The RSTA annex is guided by the ISR strategy developed while creating the joint air operations plan (JAOP).

DEPUTY CHIEF OF STAFF OF THE AIR FORCE FOR ISR AND CYBER EFFECTS OPERATIONS.

The Deputy Chief of Staff of the Air Force for ISR and Cyber Effects Operations (HAF A2/6), is the Service's Head of the Intelligence Community Element (HICE) and senior intelligence officer (SIO). HAF A2/6 represents the USAF to the national intelligence community and is the principal USAF advisor to national and DOD executives for ISR and cyber effects operations (CEO) programs and capabilities integration. As the USAF HICE, HAF A2/6 is responsible for leveraging and integrating USAF and national capabilities, collaborating with allies and partners, developing intelligence foreign disclosure policy, disseminating intelligence sharing guidance, and establishing the necessary linkages between planning and execution to integrate USAF and intelligence community capabilities.

Air Combat Command (ACC). ACC provides combat-ready intelligence forces, support, and equipment to CCMDs when directed. ACC meets this responsibility as the ISR global force manager and the lead major command for managing and modernizing numerous ISR capabilities. These ISR capabilities include the DCGS; geospatial intelligence; cyberspace intelligence; science and technology intelligence; measurement and signature intelligence; signals intelligence; and all-source analysis, targeting, and associated intelligence products.

Sixteenth Air Force (16 AF). 16 AF is subordinate to ACC and executes ISR responsibilities in support of CCMDs and combat support agencies.

USAF Service Component Intelligence (A2). The air component commander's A2 guides Service component intelligence forces by recommending policy and guidance and

ensuring coordination among various intelligence functions. The A2 is responsible for intelligence plans and programs, sensitive compartmented information management, intelligence liaison, foreign disclosure, and intelligence information management functions. The A2 is responsible for intelligence support to the air component commander and assigned or attached Service component forces. This includes the following:

- Serves as the Service component SIO. Advises the air component commander on all intelligence matters impacting mission accomplishment.
- Recommends USAF intelligence policy and guidance for operations within the joint operations area in coordination with the JFC J2.
- Establishes, coordinates, and monitors Service component intelligence requirements and capabilities to support operations.
- Coordinates and monitors JFC intelligence requirements.
- Coordinates with the JFC staff to establish joint and foreign partner relationships governing federated intelligence operations and distributed operations in theater.
- Validates unit intelligence and systems requirements and manages fielding and operation of automated intelligence systems.
- Participates in contingency planning processes and development of Service annexes to contingency plans, operational plans (OPLANs), planning orders, and operation orders.
- Assists the USAF Service Component Operations, Plans and Requirements (A3/5) in developing the air component commander's critical information requirements (CCIRs) and ensures the CCIRs are communicated to the J2 for action.
- Plans and develops instructions to implement wartime intelligence support, including augmentation of joint forces.
- Plans intelligence architecture support to satisfy Service-specific weapon system employment requirements in accordance with OPLANS.
- Establishes procedures for and manages theater production requests and RFIs.

PRESENTATION OF INTELLIGENCE FORCES

USAF intelligence forces are normally presented to JFCs through an AOC and air expeditionary task force (AETF) structure. USAF intelligence forces are sometimes employed in support of other components through joint expeditionary taskings. These taskings are Service-specific and allocated based on requests for forces submitted by a CCDR. Intelligence personnel are attached based on the skill sets required to present a capability rather than via an AETF. Similarly, the USAF conducts many peacetime intelligence operations in support of CCMDs or interagency customers that do not support a JTF and do not fall under an AETF construct. When Airmen are tasked to augment another Service, the AETF model should be applied as a template.

Most USAF ISR assets are considered high demand, low density (HD/LD) and are often tasked to perform a range of missions across the globe in support of CCMDs with an area of responsibility (AOR) as well as those with global responsibility. The Joint Staff coordinates with the Military Departments/Services, CCDRs, and intelligence agencies to identify and recommend joint global platform/sensor-based ISR and associated PED capability sourcing solutions. Some assets may be theater assigned. When emergent requirements exceed the capabilities or capacity of assigned forces, additional forces can be allocated to CCMDs by SecDef through the Global Force Management Allocation Plan (GFMAP). For both assigned and allocated forces, SecDef specifies the command relationship authorities.

REACHBACK, DISTRIBUTED, AND REMOTE SPLIT OPERATIONS

The USAF provides JFCs and air component commanders with some intelligence capabilities via reachback, distributed operations, or remote split operations. This enables the employment of ISR capabilities with a reduced, disaggregated forward footprint, further strengthening airpower's advantages by providing timely and tailored intelligence across the globe to multiple end-users. Reachback supports forward operations from a rear position, which is often more easily protected and resourced. Similarly, distributed and remote split operations provide a resiliency benefit by complicating adversary targeting. Despite these benefits, reachback and distributed operations have some limitations. Particularly, these approaches may limit face-to-face interaction and require significant communications infrastructure to support resilient data processing, exploitation, storage, and other dissemination means.

Reachback and Distributed Operations. The USAF DCGS is part of a family of systems that provide ISR planning and PED through a combination of reachback, forward support, and collaboration. Also referred to as the AN/GSQ-272 SENTINEL, the DCGS is the USAF's primary ISR PCPADE weapon system. The DCGS leverages USAF, sister Service, national, and multinational sensors in all domains to ingest information for all-source intelligence production. It provides exploitation, fusion, and dissemination for most USAF airborne imagery and signals intelligence collection. The DCGS system is scalable and capable of deployed and globally distributed operations. DCGS products are tailored for end-user requirements in specified formats, timelines, and channels.

As a networked weapon system, all DCGS sites—DGSs—are linked. This maximizes effectiveness and efficiency by leveraging workforce and intelligence resources across the enterprise and ensures continuity of operations. PED taskings are routinely transferred from one core site to another without moving intelligence personnel. The degradation of one or more core sites will not normally degrade the presentation of DCGS PED forces to the CCDR or JFC.

DCGS PED and analytical lines of effort (ALOE) are primarily tasked via the supported theater ATO and its RSTA annex. The lead DCGS wing publishes a daily PED tasking order to task DGS sites. Within each DGS, airmen are organized around problem-sets and formed into mission management teams (MMTs) and analysis and exploitation teams (AETs). MMTs are primarily responsible for driving the process to create ALOE derived from CCIRs and PIRs. Although regionally aligned to provide direct support to CCDRs,

the DCGS enterprise can adjust and focus ISR PED and ALOE capability when and where required to support DOD priorities.[10]

Remote Split Operations. Remote split operations employ forward-deployed, multi-role remotely piloted aircraft (RPA) from a home station via satellite links, thereby reducing the forward-deployed footprint. With the bulk of mission crew resources and communications architecture reserved stateside or in rear areas, this employment model provides a unique capability to rapidly transition RPA aircrew between missions across the globe in response to dynamic and changing requirements.

As with other HD/LD assets, USAF RPA combat lines are assigned to CCMDs at the SecDef level through the GFMAP. Generally, CCDRs maintain OPCON of in-theater aircrew, aircraft, and support equipment, and are delegated TACON of the remote mission crew controlling a theater assigned aircraft. With SecDef approval or prior authorization, CCMDs may coordinate to shift mission crew capacity from one AOR to another when a short-term, excess capacity in the losing AOR results from either weather or maintenance related issues.

INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE DIVISION

The AOC provides operational-level command and control of air component forces as the focal point for planning, executing, and assessing air component operations. Within the AOC, the ISRD integrates the JFC's theater-wide intelligence capabilities to include distributed support. Central functions of the ISRD include planning, collection management, and analysis.

The ISRD is responsible for orienting the air component commander to current and emerging enemy capabilities, threats, courses of action, and center(s) of gravity; intelligence operations management; and targeting intelligence support. The ISRD accomplishes these tasks by integrating intelligence operations with the ATO. This integration provides crucial intelligence to the air mobility, strategy, combat plans, and combat operations division as operations are planned and executed. Additionally, the ISRD supports planning, tasking, and execution of theater air and cyberspace intelligence operations. The ISRD is the senior intelligence element of the theater air control system and integrates ISR platforms and capabilities, ensuring they are managed optimally within the context of national, joint, and combined intelligence architectures. The ISRD chief (CISRD) is the SIO for the AOC, reports to the AOC director, and works closely with other AOC division chiefs and senior staff to determine the best use of intelligence personnel. In addition, the CISRD works closely with the A2 to ensure ISRD and A2 staffs work together effectively. The ISRD:

- ✪ Provides the air component commander, staff planners, AOC divisions, and other USAF elements in the theater with a common threat picture and analysis of adversaries.

[10] Current as the time of this publication, the 480th ISRW is the lead DCGS Wing. The Air Force Special Operations Command (AFSOC) DCGS is tasked through AFSOC or through the ISR tasking process.

- Provides combat intelligence support assessment activities for air component operations planning and execution in conjunction with the strategy, combat plans, and combat operations divisions.
- Directs and manages the air component's intelligence operations, including reachback, distributed, and federated operations.
- Provides direct targeting support to the ATO cycle.
- Provides all-source intelligence support to other AOC divisions to enhance the execution of their core processes.

INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE DIVISION ROLES

Analysis. Within the ISRD, analysis functions support the joint intelligence preparation of the operational environment (JIPOE), intelligence preparation of the battlespace (IPB)[11], and developing assessments that enhance friendly understanding of the operational environment and adversary intentions and behaviors. Intelligence analysts synthesize intelligence and data; apply critical thinking; identify, assess, and fill intelligence gaps; and conduct predictive analysis.

ISR Operations and Collection Management. ISRD intelligence operations include collection management for theater airborne ISR requirements, planning theater airborne ISR operations, and associated PED. The ISRD is the optimal entity for COM of theater airborne ISR operations. To ensure ISR operations align with air component commander objectives, intelligence operations planners and collection managers attend joint collection working groups and management boards to advocate for air component collection priorities based on PIRs, RFIs, targeting requirements, and other intelligence needs.

Target Development and Battle Damage Assessment. The ISRD is responsible for target development and battle damage assessment (BDA). Target development includes evaluating and nominating potential adversary targets based on commander's guidance and intended effects. In addition, BDA facilitates reporting on physical and functional damage and change assessments post-strike. The ISRD also supports munitions effectiveness assessments and restrike recommendations.

Unit Support. The ISRD provides USAF unit support by liaising with wing-level CINs. Unit support functions include oversight of theater intelligence reporting procedures, the RFI process, and additional unit intelligence requirements. These functions include receiving and processing mission reports and RFIs from USAF units.

[11] The term intelligence preparation of the battlespace has been removed from the DOD Dictionary. Content related to the term has been moved to the *Joint Guide for Joint Intelligence Preparation of the Operational Environment*.

INTELLIGENCE PERSONNEL ACROSS THE AIR OPERATIONS CENTER

USAF intelligence personnel are embedded in other AOC divisions and staff elements, and across the broader theater ISR Enterprise to integrate intelligence in the planning cycle and to support command and control of theater air and cyberspace forces.

Strategy division. Intelligence personnel in the strategy division assist in developing the air component strategy, JAOP, and air operations directive (AOD). Intelligence analysts provide JIPOE products, coordinate with ISR teams to develop PIRs, and ensure PIRs are included in the JAOP and AOD. Collection experts advise on available intelligence assets and capabilities and develop the ISR strategy as part of the overall air component strategy.

Strategy division targeteers use intelligence products for target system analysis (TSA) products. They continuously update the TSA assessment and assist the development of objectives, tasks, and measures of effectiveness, and provide combat assessment inputs (BDA, munitions effectiveness, and mission assessment) that feed into the tasking cycle.

Combat plans division. Intelligence personnel in combat plans enable theater air and cyberspace operations by ensuring intelligence operations are linked to commander objectives. ISRD analysts provide continually updated JIPOE analysis and generate RFIs as needed to respond to specific requirements of the planning and tasking processes. Targeteers work closely with the combat plans staff judge advocate to validate targets for inclusion in the draft joint integrated prioritized target list consistent with objectives, guidance, rules of engagement, and the law of war. In addition, intelligence planners ensure the integration of intelligence operations into the tasking process by coordinating asset inclusion in the master air attack plan (MAAP) and the RSTA annex, to focus priorities, weight of effort, and intended goals.

Combat operations division. Intelligence personnel within the combat operations division form the senior intelligence duty officer (SIDO) team. This team provides up-to-date intelligence inputs and situational awareness for the chief of combat operations. In addition, the SIDO leads current intelligence operations to maintain an accurate threat picture, support dynamic operations (e.g., personnel recovery and dynamic targeting), and monitor the ATO and RSTA execution. The SIDO team coordinates with platform and PED liaison officers for dynamic retasking of theater air and cyberspace ISR assets and PED support to meet JFC objectives.

Air mobility division. Intelligence personnel in the air mobility division ensure air mobility missions operate with a common intelligence picture and assess the impact of threats on air mobility planning, execution, and force protection. In addition, assigned intelligence personnel provide tailored intelligence products to support air mobility operations and coordinate efforts with intelligence personnel at Air Mobility Command and the 618th Air Operations Center (Tanker Airlift Control Center) for inter-theater US Transportation Command airlift missions operating in theater.

ISR liason officers. ISR liaison officers (ISRLOs) support AOCs and other organizations conducting supported operations. They can be integrated with other components at

operational and tactical levels to advise, assist, and educate aligned supported units on AF ISR assets while in-garrison or deployed. They provide recommendations on integrating and synchronizing DCGS and other intelligence capabilities into theater operations. As a USAF ISR subject matter expert, ISRLOs act as a conduit for intelligence requirements between supported commanders, intelligence staffs, ISRD analysts, DGS, and other reachback organizations. Additionally, ISRLOs increase situational awareness by providing details on current operations to intelligence crews. This two-way feedback provides AOCs and other reachback organizations insight into the operations they support to enhance the operational assessment of ISR.

CHAPTER 3: INTELLIGENCE PROCESS

Intelligence and operational requirements drive the planning and execution of intelligence operations. Intelligence requirements begin at the national or strategic level. From there, the air component commander or their staff establish operational level requirements, which are then tailored and refined to the tactical level. ISR operations collect data on these focused requirements. Collected data is then used to produce intelligence through the joint intelligence process to meet intelligence requirements. Understanding these requirements and where they come from is the linchpin to successful planning and execution. For more information on intelligence disciplines, see Appendix B.

INTELLIGENCE REQUIREMENTS

COMMANDER'S CRITICAL INFORMATION REQUIREMENTS

Intelligence support to the air component commander CCIRs includes the development of PIRs and essential elements of information (EEI) following the method outlined in JP 2-0, *Joint Intelligence*, during the joint planning process for air (JPPA). The air component commander establishes CCIRs to identify information requirements that are critical to facilitate timely decisions. The two key elements of CCIRs are friendly force information requirements (e.g., operational status of ISR assets) and PIRs. ISR activities supporting CCIRs should be coordinated with the servicing judge advocate to ensure compliance with the law and any existing rules of engagement.

PRIORITY INTELLIGENCE REQUIREMENTS

During intelligence planning and direction, intelligence planners identify the intelligence required to answer CCIRs. Intelligence requirements deemed most important to mission accomplishment are identified as PIRs. PIRs are general statements of intelligence needs. They provide the framework to prioritize all intelligence operations within a CCMD and ensure efforts are focused on critical information needed to support warfighters. PIRs are driven by, and in turn drive, the JIPOE process to refine information requirements and support command decisions. Examples of PIRs include such things as, "What is the operational status of the adversary's integrated air defense system?", or "What terrorist groups are active within the area of responsibility?"

ESSENTIAL ELEMENTS OF INFORMATION

PIRs drive the development of detailed EEIs. EEIs further refine PIRs by outlining specific information requirements—i.e., "What is the current location of the adversary SA-20 battery?" EEIs are linked to PIRs to ensure intelligence operations focus on commander priorities. As commander direction and guidance evolve, planners may develop new EEI requirements or modify existing requirements.

REQUESTS FOR INFORMATION

RFIs are used to task and manage intelligence analysis requirements to answer CCIRs and PIRs. RFIs may be submitted and coordinated across the intelligence community when the necessary analysis cannot be performed within a tasked organization.

INTELLIGENCE PROCESS ACTIVITIES

The joint intelligence process provides the basis for common intelligence terminology and procedures. It comprises six interrelated categories of intelligence operations. These categories are characterized by broad activities conducted by intelligence staffs and organizations to provide commanders and national-level decision-makers with relevant and timely intelligence. The six categories of intelligence operations are planning and direction; collection, processing and exploitation; analysis and production; dissemination and integration; and evaluation and feedback.[12]

PLANNING AND DIRECTING

Within the AOC, the intelligence process begins in strategy development. The ISR strategy, annotated in the JAOP and AOD, is synchronized with theater and national strategies and defines the roles ISR and intelligence capabilities will play in achieving operational objectives. Further, it provides the foundation to develop and validate intelligence requirements, establishes the framework for planning and directing ISR operations, and guides execution of the ISR processes. During strategy development, planners should determine appropriate evaluation and feedback measures to enable accurate operational adjustments or shifts in follow-on strategies.

During intelligence planning, intelligence requirements are determined, appropriate intelligence architectures are developed, and collection plans are prepared. To make the planning process more efficient, information requesters should clearly articulate collection requirements. Precise requirements allow collection managers and operations planners to determine the best way to meet requirements.

The ISRD coordinates and executes C2 of ISR activities through the combat operations division and the SIDO to ensure synchronization and integration. When applicable, these activities are directed via the ATO and its RSTA annex.

COLLECTION

Collection refers to operations and activities that acquire and provide information to processing elements by tasking appropriate assets or resources that acquire the data and information required. Collection includes identifying, prioritizing, coordinating, and positioning assets or resources to satisfy intelligence requirements. Many airborne ISR assets used in collection can be based or launched from airfields outside an area of interest, enabling collection to be conducted without need for a significant forward footprint, thereby presenting potential operational advantages in some circumstances.

[12] For additional information on the intelligence process, see JP 2-0.

PROCESSING AND EXPLOITATION

Once data is collected, it is processed and exploited. Processing and exploitation requirements are prioritized and synchronized with the commander's PIRs. Collected data is correlated, converted into a suitable format, and transformed into information that can be readily disseminated, used, exploited, transmitted, stored, and retrieved by intelligence analysts for subsequent analysis and intelligence production.

Processing and exploitation remain distinct from analysis and production. Though the information produced is analyzed for time-critical production, it is not subjected to full all-source analytical assessment. Relevant time-sensitive information produced in this step (i.e., targeting, personnel recovery, or threat warning information) should be immediately disseminated through theater and global intelligence broadcasts, intelligence reporting and messaging systems, imagery product libraries, intelligence databases, or message reporting.

ANALYSIS AND PRODUCTION

During analysis and production, processed and exploited data is converted into intelligence by integrating, evaluating, analyzing, and interpreting all-source data to produce intelligence products in support of known or anticipated user requirements. Integrated, all-domain, ISR-generated data can provide an understanding of demographics, culture, physical terrain, centers of gravity, and financial, social, and political infrastructures.

Analysis and production are accomplished through a structured series of actions that typically occur in sequence. In some cases, they may also be conducted concurrently. Conducted in response to existing or anticipated intelligence production requirements, these steps include:

- **Integration.** Information is received, collated, and entered into appropriate databases by intelligence organization analysis and production elements, the theater joint intelligence operations center (JIOC), or other joint or component elements such as the ISRD. Information is integrated and grouped with related pieces of data according to predetermined criteria to evaluate newly received information.

- **Evaluation.** Each new item of information is evaluated by the appropriate analysis and production element with a focus on a source's reliability and credibility. To avoid bias, the reliability and credibility of each source should be assessed independently.

- **Analysis.** During analysis, integrated and evaluated information is compared with known facts and predetermined assumptions to form assessments. These assessments are combined and evaluated to discern patterns, links, or recognized events. Analysis can also identify opportunities or knowledge gaps that drive future collection. Analytic fundamentals typically include the activities of discovery, assessment, explanation, anticipation, and delivery. Example analytical outputs include but are not limited to spatial and temporal, network, trend, and forensic-based.

- **Interpretation.** Interpretation is an inductive process in which information is judged in relation to existing information and intelligence. It involves identification of new activities and decisions regarding the significance of those activities.

Activity-Based Intelligence

Activity-based intelligence is an approach to activity and transactional data analysis that rapidly integrates data from multiple sources around the interactions of people, events, and activities to discover relevant patterns, determine and identify change, and characterize those patterns. Activity-based intelligence can be leveraged to resolve unknowns, develop object and network knowledge, and drive collection.

Intelligence fusion. Execution of these steps enables intelligence fusion—a process that examines all sources of intelligence and information to derive a comprehensive assessment of activity. Collaboration enables intelligence analysts to share information, discuss opinions, debate hypotheses, and identify or resolve analytical disagreements. Efforts to produce fused intelligence can be bolstered through the establishment of collaborative environments and structures that provide access to recognized experts. This is especially important when the units and experts involved are geographically separated.

Advances in network capabilities greatly enhance analysts' ability to share, compare, and assess information. As databases grow in volume and complexity, potentially vital pieces of information may become increasingly difficult for analysts to find and retrieve. Virtual knowledge bases have been designed to serve as integrated repositories of multiple databases, reference documents, and open-source material to overcome this find and retrieve limitation.

DISSEMINATION AND INTEGRATION

The dissemination and integration step involves the delivery to and use of intelligence. Dissemination ensures commanders, planners, and operational forces receive finished intelligence in time to make effective decisions and execute operations. The USAFs' distributed operations capability provides timely and tailored intelligence across the globe to multiple end-users.

Dissemination is accomplished through various means, each requiring continuous management (e.g., electronic transmission, hardcopy annotated imagery and maps, direct threat warnings, oral and written reports, briefings, and various servers allowing structured discovery and retrieval). When managed ineffectively, communications paths can become saturated by information retransmitted by numerous intermediate collection agencies, resulting in circular reporting. Advances in cyberspace capabilities and technologies should be leveraged to improve dissemination and reduce the information-to-production timeline for delivery of intelligence products. Importantly, intelligence planning should include procedures for rapidly coordinating with public affairs for the public release of appropriately declassified intelligence.

Integration ensures disseminated intelligence is employed effectively. After intelligence products have been disseminated, intelligence organizations are responsible for continuing to support users as they integrate the intelligence into decision-making and planning processes. Continuous integration of intelligence and operations allow commanders and operational planners access to the most current information. This access optimizes intelligence support to operations planning, preparation, execution, and assessment functions.

EVALUATION AND FEEDBACK

All operations in the intelligence process are interrelated and should be evaluated to determine the degree to which they facilitate each other and succeed in meeting intelligence requirements. Importantly, evaluation and feedback are not an independent operation in the intelligence process. Rather, it should be conducted continuously to assess the intelligence process. The goal is to identify issues as early as possible to minimize information gaps, mitigate capability shortfalls, and ensure intelligence operations meet established analysis tradecraft and objectivity standards.

Evaluation and feedback require a collaborative dialogue between intelligence planners, collection managers, collectors, and analysts to identify deficiencies within the intelligence process. Assessment of intelligence operations relies on product satisfaction, as determined by the user. As such, intelligence personnel and users should provide timely feedback regarding intelligence process successes and problems. A formalized process should be established to ensure feedback is provided consistently and analyzed systematically.

Assessment. An ISR strategy is not complete unless it includes a qualitative and quantitative ISR assessment.[13] Assessments provide leaders with information to reprioritize intelligence requirements, shift collection emphasis, change analytic levels of effort, and reallocate available ISR assets. To perform assessments of intelligence activities and operations, intelligence planners develop and document intelligence measures of performance (MOPs) and intelligence measures of effectiveness (MOEs). MOPs are informed by quantitative indicators. They indicate whether a particular platform or sensor is performing as expected: e.g., the number of sorties conducted or number of images taken. Conversely, MOEs gauge the impact of intelligence tasks performed within the intelligence process. MOE indicators tend to be qualitative and related to the value of the intelligence produced.[14]

METHODOLOGIES AND PRODUCTS

Various intelligence methodologies and products are used to provide predictive analysis, real- and near-real-time threat assessment, and target and friendly forces status to commanders, staffs, and operational units. Products are tailored via formal reporting methods,

[13] For additional information on ISR assessments, see AFTTP 3-2.88, *Multi-Service Tactics Techniques and Procedures for ISR Optimization.*
[14] For additional information on assessment, MOEs, and MOPs, see AFDP 3-0, *Operations and Planning*, JP 5-0, *Joint Planning*, and JP 2-0.

informal or formal briefings, background papers, annotated imagery, graphic or video presentations, dynamic databases, and near-real-time displays. The following are some of the methodologies and products that contribute to situational awareness.

INTELLIGENCE PREPARATION OF THE OPERATIONAL ENVIRONMENT

JIPOE and IPB are key tools for analysis and production that support joint planning and inform decision-makers at all echelons about emerging situations and threats. However, JIPOE and IPB differ significantly in purpose and scope. JIPOE supports the JFC and is conducted by intelligence personnel within CCMDs and joint forces. This macro-analytic approach considers cultural, social, religious, economic, and government factors but is focused on determining adversary intent, whole-of-government options, centers of gravity, and strategic vulnerabilities.

In comparison, IPB is conducted by intelligence personnel within Service and functional components and supports the individual operations of the component commands with force-specific micro-analysis. JIPOE and IPB complement one another in their separate roles, ultimately assisting commanders in determining where and when to focus attention to influence events, ready forces, and begin setting conditions for future operations.

WARNING INTELLIGENCE

Warning intelligence products are derived from a worldwide system that analyzes and integrates information to assess the probability of hostile actions and provide sufficient warning to preempt or counter their effects. Warning intelligence systems rely on information and indications from sources at all levels. The focus of warning intelligence products varies at each echelon and is most specific at the operational and tactical levels. In general, warning intelligence products focus on the following:

- Emerging crises and foreign government responses to them.
- Potential adversary political and military intentions, past behaviors, motivations, and doctrine.
- Significant political, economic, or social situations, in both friendly and adversary states that may potentially trigger crises.
- Changes in adversary force dispositions, military activities, and mobilization status.
- Adversary disinformation capabilities.
- Civil or bureaucratic activities that may suggest subsequent military activity.
- The status of other military forces in an operational area.

CURRENT INTELLIGENCE

Current intelligence is produced by fusing data and intelligence products regarding the current situation in a particular area or the activities of specific groups. This type of intelligence is similar to warning intelligence in that both require continuous monitoring of

world events and specific activities in an operational area. Information required to produce current intelligence products includes, but is not limited to, the following:

- Adversary intentions, capabilities, and will to use military force or other instruments of national power.
- An adversary's potential centers of gravity, operational plans, and vulnerabilities.
- Geographic, environmental, and social analysis of the operational area.
- Significant military and political events.
- Status of strategic transportation nodes (e.g., major airfields, seaports, and cyberspace capabilities architecture).
- Analysis of weapons of mass destruction threats against the US, its allies, and partner nations.
- Disposition of adversary forces (DOF).

GENERAL MILITARY INTELLIGENCE

General military intelligence (GMI) is intelligence concerning foreign countries' military capabilities or topics affecting potential US or multinational military operations. Current intelligence and GMI form a symbiotic relationship. Information gained during the development of current intelligence forms the basis for the GMI effort and other analytical products. Conversely, GMI provides underlying threat information to produce accurate and meaningful current intelligence.

GMI focuses on military capabilities, including:

- Order of battle, organization, DOF, training, tactics, doctrine, strategy, and other factors bearing on military strength and effectiveness.
- Transportation capabilities.
- Military materiel production and support industries.
- Military and civilian communications systems.
- Military economics, including foreign military assistance.
- Use of asymmetric tactics or terror attacks.
- Location, identification, and description of military-related installations.

The following are examples of GMI products:

- **Military-related Infrastructure Assessments.** These assessments provide detailed indicators of an adversary force's capabilities and vulnerabilities, including its warfighting sustainability.

- **Military Capabilities Assessments.** Determining the adversary's potential military capability includes identifying DOF and their readiness levels, evaluating vulnerabilities, and assessing adversary abilities to employ military force.

TARGET INTELLIGENCE

Intelligence operations play a prominent role in the targeting cycle by detecting, locating, and identifying targets and supporting mission planning and assessment. Target intelligence portrays and locates the components of a target or target complex and indicates its vulnerability and relative importance. Required products, such as target imagery, should be immediately available to support the ATO and mission planning cycles. ISR assets may be employed to detect and identify potential targets, changes to existing targets, or to conduct battle damage assessment. Multiple missions may be required to provide the level of detail necessary to support the precision engagement of specific targets. Target intelligence products include annotated target graphics, electronic target folders, target system analyses, and geospatial information to provide comprehensive data needed to plan and deliver lethal and nonlethal effects.

SCIENTIFIC AND TECHNICAL INTELLIGENCE

Scientific and technical intelligence (S&TI) examines foreign developments in basic and applied sciences and technologies with potential for military use, particularly to enhance weapon systems. S&TI is a product that results from collection, evaluation, analysis, and interpretation of foreign scientific and technical information. It covers the following:

- Foreign developments in basic applied research and applied engineering techniques.
- Scientific and technical characteristics, capabilities, and limitations of foreign military systems, weapons, weapon systems, and materiel; the research and development related to it; and the methods used to manufacture them.

Example S&TI products include weapon system characteristics, capabilities, vulnerabilities, limitations, effectiveness, research and development, and related manufacturing information. S&TI products play a vital role in the acquisition process by allowing the procurement of systems or systems upgrades to meet current, developing, and future threats.

Acquisition intelligence. Acquisition intelligence addresses future threats, specializing in S&TI to anticipate enemy capabilities in advance by one to five years. Acquisitions intelligence brings a focus on supportability issues associated with new ISR capabilities planned to be brought into theater. It is especially important for coalition operations.

COUNTERINTELLIGENCE

CI includes strategic analysis to identify and produce all-source finished intelligence on foreign intelligence threats to friendly operations. CI develops and implements strategies and action plans to counter the CI threat, tasks CI collection capabilities, and leverages all other intelligence disciplines to fill CI collection gaps.

CI is critical to USAF operations, particularly force protection efforts. CI threat estimates and vulnerability assessments identify friendly weaknesses and vulnerabilities that may be exploited by an adversary. CI supports friendly planning efforts through sociocultural analysis of enemy leadership characteristics. CI can also help assess enemy reactions to friendly deception efforts. Various classified CI databases maintain information on personalities, organizations, installations, and incidents. These databases can help provide indications of the motivations and ideology of potential adversaries.

AFOSI is the sole authorized executor of the CI mission for the Department of the Air Force (DAF). No other DAF entities are authorized to conduct CI activities. AFOSI is a field operating agency under the administrative guidance and oversight of the Air Force Inspector General (SAF/IG). AFOSI forces normally operate in a Service retained status under the Commander, AFOSI. When attached to a CCMD, as specified by a military operation or operation order, the exercise of CI authorities may be under the OPCON of a CCDR providing a CI capability in support of CCDR PIRs. CCDR CI authority may limit AFOSI's ability to conduct Service CI activities. The Secretary of the Air Force (SecAF) retains administrative control (ADCON) for those USAF CI resources under OPCON of the CCDR.

ESTIMATIVE INTELLIGENCE

Estimative intelligence provides forecasts of current or potential situations that may have bearing on the planning and execution of military operations, otherwise known as estimates. By employing pattern analysis, inference, and statistical probability techniques, intelligence personnel produce estimates describing relevant actors' capabilities and behavior.

IDENTITY INTELLIGENCE

Identity intelligence results from the fusion of identity attributes (biologic, biographic, behavioral, and reputational information related to individuals), and other information and intelligence associated with those attributes, collected across various intelligence disciplines. The goal of identity intelligence is to discover unknown potential threat actors by connecting individuals to other persons, places, events, or materials; analyzing patterns of life; and characterizing the threat they pose to US interests.

APPENDIX A: INTELLIGENCE RESOURCES

Understanding collection resources ensures effective allocation of assets to meet intelligence requirements. Importantly, some of the systems annotated here provide inputs to intelligence operations but are not dedicated intelligence resources or systems.

AIRBORNE SYSTEMS

Airborne ISR can provide a unique, taskable, and visible presence to provide real-time, tailorable information during mission execution. Airborne platforms can cover a large area with a mix of sensors. Additionally, most of these assets have a common data link between aircraft or ground stations, allowing them to distribute large volumes of information in near-real-time. Planners should consider the required PED support needed for various airborne ISR assets and leverage reachback if additional PED is needed. Requirements for PED between wartime and peacetime may vary. During peacetime, most airborne intelligence missions are accomplished using standoff techniques. A standoff mode is also used during military operations when the threat is too significant to allow high-value assets to penetrate adversary territory or when the overflight of an area cannot be completed due to political sensitivities. Though employment of standoff techniques may mitigate enemy surface-to-air and air-to-air threats, it also limits range and depth of sensor coverage.

Non-traditional ISR. Increasingly, ISR planners and collection managers may find that the capacity of traditional ISR-only assets is insufficient to satisfy all collection requirements. When developing collection plans, ISR planners should be mindful that available resources are not limited to specific platforms or sensors. Collection managers should understand how to integrate non-traditional ISR (NTISR) assets—assets capable of conducting reconnaissance or surveillance to varying degrees, even if ISR collection is not their primary mission. One method for employing NTISR is operations reconnaissance (ops recce), a tactic to deliberately leverage strike aircraft sensors to increase battlespace awareness and lethality beyond their original purpose.

Depending on the operation, NTISR assets can be called on to provide a wide range of ISR collection support. ISR planners should understand the broad range of capabilities and limitations associated with specific aircraft and articulate the information and data assets can provide. Additionally, the availability of these assets may be sporadic. Collection managers should be proactive and take advantage of capabilities when they are available. To task NTISR assets, collection managers should coordinate with operations personnel in the respective AOC's combat plans, or combat operations division to task NTISR assets.

Mission Authorities. Roles and missions for many USAF assets have expanded beyond what was envisioned in their initial employment concepts. It is not unusual to find strike aircraft employed in an ISR role. Whether the aircraft is dedicated to conduct ISR for an entire mission or just a portion, mission objectives, priorities, and guidance for multi-role aircraft employment, and the authority to task the weapon system, should be clear and developed in advance of mission execution**.** The air component commander should

ensure the following authorities are defined to ensure clear lines of control during multi-role missions:

- **Aircraft Control:** The individual in authority and technically capable of controlling the aircraft. In almost all cases, authority over aircraft operation is vested with the designated pilot-in-command (PIC). PIC authority covers all aspects of aircraft operation, including onboard equipment and sensors.[15]
- **Sensor Control:** The organization or individual in authority and technically capable of controlling the aircraft sensor(s).
- **Sensor Tasking:** The organization with authority to task aircraft sensors. Sensor taskings should provide direction on what is to be accomplished, not how.

SPACE-BASED SYSTEMS

Space-based intelligence systems are integral to military operations. Space systems provide information to commanders allowing them to quickly assess the situation, develop concepts of operation, and distribute changes to their forces. The primary advantage of space-based systems is their global and wide-area coverage over denied areas where ground and airborne sources are limited. Other advantages include mission longevity and reduced vulnerability to adversary action. While able to provide worldwide coverage, demands on individual space-based systems often exceed their capacity. Their associated orbit requirements may limit the ability to meet operational requirements. Additionally, space-based ISR can be limited by advanced denial and deception techniques. Cooperation with allies and other partners on military space-based ISR systems may contribute to US national security objectives by enhancing interoperability, supporting multinational operations, and building partnership capacity.

Military space-based systems. Military space-based systems employ a variety of sensor suites and provide a broad range of capabilities. During peacetime, space systems routinely support training exercises, peacekeeping operations, indications and warning, disaster and humanitarian relief efforts, counterterrorism, and counterdrug operations. Environmental monitoring systems provide an asymmetric advantage in by enabling the anticipation and exploitation of ocean, soil, atmosphere, and space environment conditions in support of friendly military operations while denying those same advantages to adversaries. Likewise, space-based ISR systems provide military forces with geographic and detailed terrain information to enhance mission planning capabilities. These systems can often cue or are cued by other ISR systems to watch a specific area of interest, enhancing accuracy and reaction times for the users of that information.

Non-military space-based systems. Non-military space-based systems can complement military space systems and include civil, commercial, and allied assets. These systems possess various capabilities; however, their availability may be limited in some cases. Often, arrangements are made for military personnel to have access to non-

[15] For additional information on PIC authority, see Air Force Manual (AFMAN) 11-202 Volume 3, *Flight Operations.*

military assets. These arrangements are often subject to legal review and take time to activate. Ideally, space system requirements should be addressed before military operations.

National satellite systems. National satellite systems are controlled by the US intelligence community and support the President, Secretary of Defense, and the military at all levels. These resources provide data and are responsive to military information needs. These systems are a limited resource. Requirements for them should be worked in advance, and detailed justification for their use should be provided. The air component submits geospatial intelligence (GEOINT) collection requirements through the CCMD J2. HAF A2/6 has delegated authority for all other USAF GEOINT collection requirements to the USAF Departmental Requirements Office.

GROUND-BASED SYSTEMS

Worldwide ground-based systems are equipped and tasked to collect information for intelligence disciplines such as SIGINT and measurement and signature intelligence (MASINT). These systems may satisfy national, theater, or local information requirements.

Air surveillance and target acquisition radars. Air surveillance and target acquisition radars used to control the movement of aircraft can also provide threat warning within a designated area. Though useful as an additional layer of control and observation, these systems are limited by adverse atmospheric conditions and susceptible to electronic jamming. Additionally, air defense sensors are limited to line-of-sight surveillance.

Missile warning and space surveillance. The space surveillance network (SSN) and ground-based missile warning sensor system offer a significant ground-based ISR resource. Ground-based missile warning sensors' primary function is to identify and characterize ballistic missile attacks on the US and its allies. They also contribute to space surveillance. The SSN aims to find, fix, track, and characterize artificial objects in space. SSN data is used to determine adversary space order of battle, adversary spacecraft overflight warning, and adversary spacecraft status. This information is available to theater commanders and provides them an early warning and additional information that can be used for denial and deception techniques.

CYBERSPACE-BASED SYSTEMS

Cyberspace-based ISR capabilities are integral to military forces and enable operations across the competition continuum. Cyberspace-focused ISR includes digital network analysis and intelligence support to USAF cyberspace missions. Additionally, specialized units provide timely and actionable all-source ISR services and products supporting national cyberspace operations. This support is generally characterized by five cyberspace focused ISR areas: current intelligence and reporting; indications and warning, threat attribution and characterization; JIPOE; and computer network exploitation under national intelligence and US Cyber Command authorities.

APPENDIX B: INTELLIGENCE DISCIPLINES

Intelligence operations are commonly organized around intelligence disciplines. Each discipline has an intelligence community (IC) and DOD functional manager. Air component intelligence should coordinate upward with the JTF J2 through the CCMD J2 to IC agencies to ensure collection elements use appropriate reporting methods with a response time sufficient to meet air component commander requirements. For additional guidance on planning, executing, and assessing various intelligence disciplines, reference AFTTP 3-2.88, *ISR Optimization*.

- **GEOINT**–Geospatial intelligence.
- **IMINT**–Imagery intelligence.
- **HUMINT**–Human intelligence.
- **SIGINT**–Signals intelligence.
- **COMINT**–Communications intelligence.
- **ELINT**–Electronic intelligence.
- **FISINT**–Foreign instrumentation signature intelligence.
- **MASINT**–Measurement and signature intelligence.
- **OSINT**–Open-source intelligence.
- **TECHINT**–Technical intelligence.
- **CI**–Counterintelligence.

GEOSPATIAL INTELLIGENCE

GEOINT is the exploitation and analysis of imagery and geospatial information to describe, assess, and visually depict physical features and geographically referenced activities on or about the Earth. GEOINT consists of imagery, imagery intelligence (IMINT), and geospatial information. GEOINT data sources include commercial satellites, government satellites, aircraft, maps, commercial databases, census information, global positioning system waypoints, and utility schematics. GEOINT can synthesize intelligence and data into conceptualized geographic spatial content that can provide commanders key operational intelligence (e.g., best vantage point for shooters, most advantageous entry points, and spatial trends and patterns). The National Geospatial Intelligence Agency (NGA) serves as the IC and DOD functional manager for GEOINT.

Imagery Intelligence. IMINT is the technical, geographic, and intelligence information derived through interpreting or analyzing imagery and collateral materials. IMINT includes the exploitation of imagery data derived from electro-optical, radar, infrared, multi-spectral, and laser sensors. IMINT results from the processing and exploitation of raw imagery (information) to create an analyzed product (intelligence). IMINT is used for historical

comparisons, to locate adversary military forces and facilities, and to provide insight into the adversary's capabilities. IMINT is also valuable for understanding the physical terrain and human aspects like significant cultural sites (e.g., government structures, historical sites, and schools), agriculture and urban infrastructure, water, electrical grids, etc. The air component should leverage the Imagery Support Element (ISE) specialty team in the ISRD for imagery production, tailored analysis, and/or exploitation.

HUMAN INTELLIGENCE

HUMINT is an intelligence collection discipline that uses people in an area of interest to identify or provide insight into adversary plans and intentions, research and development, strategy, doctrine, and capabilities. Dedicated HUMINT collectors amplify, clarify, or verify information collected by other airborne, ground-based, or space-based assets. In many cases, HUMINT may be the best source regarding adversary intentions. The USAF has an organic HUMINT capability and works with DOD and other national-level agencies to collect on priority USAF operational and strategic requirements. The Director of the Central Intelligence Agency (CIA) serves as the National HUMINT Manager, and the Director of the DIA serves as the DOD functional manager.

SIGNALS INTELLIGENCE

SIGINT is a category of intelligence comprised of COMINT, ELINT, and FISINT, that may consist of an individual element, or a combination. SIGINT uses intercepted electromagnetic emissions to provide information on adversary forces' capabilities, intentions, formations, and locations. SIGINT also includes collecting, processing, and exploiting data from information in cyberspace. The air component's link to the SIGINT enterprise is the National Tactical Integration (NTI) specialty team in the ISRD. The NSA serves as the IC functional manager for SIGINT.[16]

Communications Intelligence. COMINT consists of information derived from intercepting and monitoring the adversary's communications systems. COMINT exploits an adversary's communications, revealing capabilities, intentions, perceived vulnerabilities, and, often, an adversary's perception of the US and multinational partners.

Electronic Intelligence. ELINT is intelligence derived from interception and analysis of non-communications emitters, such as radars. ELINT includes both operational electronic intelligence (OPELINT) and technical electronic intelligence (TECHELINT). OPELINT focuses on operationally relevant information (location, movement, employment, tactics, and activity of foreign non-communications emitters and associated weapons systems). TECHELINT concentrates on the technical aspects (signal characteristics, modes, functions, associations, capabilities, limitations, vulnerabilities, and technology levels).

Foreign Instrumentation Signature Intelligence. FISINT consists of technical information derived by intercepting electromagnetic emissions associated with testing and operational deployment of foreign air and space, surface, and subsurface systems. These

[16] For additional information on the role of NTI, see AFTTP 3-1.NTI, *National Tactical Integration* (found on the joint worldwide intelligence communication system [JWICS]).

emissions are typically generated by telemetry, electronic interrogators, and video data links. The technical details of foreign weapons system development derived from FISINT can provide insight into foreign capabilities, identify avenues for exploitation, and/or aid the employment of appropriate countermeasures. FISINT is accomplished by specialized, national-level Service and DOD organizations.

MEASUREMENT AND SIGNATURE INTELLIGENCE

MASINT is technically derived intelligence to detect, locate, and describe the physical measurements and signatures intrinsic to targets and events. MASINT collects and produces precise threat characteristics and performance information essential to support planning, development, and application of weapon systems, countermeasures, targeting, and battle damage assessment. MASINT is especially useful to monitor adversary technical developments and deployments, as well as emerging threats from weapons of mass destruction. DIA leads the IC effort for MASINT via senior science and technology officers (SSTOs) who integrate DIA efforts to meet operational intelligence requirements.

OPEN-SOURCE INTELLIGENCE

OSINT is intelligence derived from publicly available information (PAI) that is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement. PAI is information that has been published or broadcast for public consumption, available on request to the public, accessible online, could be seen or heard by a casual observer, or obtained by visiting a place or event open to the public. OSINT complements other intelligence disciplines and may cue collection and analysis, fill intelligence gaps, and supplement the accuracy and fidelity of classified information databases. Importantly, OSINT is susceptible to manipulation and deception and requires research expertise and OPSEC for internet-based activities. The Director of the CIA is the IC functional manager for OSINT and the DIA Director is the DOD's functional manager.

TECHNICAL INTELLIGENCE

TECHINT is intelligence produced by collecting, processing, analyzing, and exploiting data and information regarding foreign equipment to prevent technological surprise, assess foreign scientific and technical capabilities, and develop countermeasures to neutralize an adversary's technological advantages. TECHINT begins with the acquisition or recovery of a foreign piece of equipment or foreign scientific or technological information. This work is typically performed in a forward-deployed location by a joint captured materiel exploitation center (JCMEC) managed by DIA and OPCON to the CCMD.

COUNTERINTELLIGENCE

CI consists of information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, persons or their agents, or international terrorist organizations or activities. CI includes both offensive and defensive operations to protect vital US national security-related information from being

obtained or manipulated by an adversary's intelligence organizations, activities, and operations. CI works closely with intelligence, security, infrastructure protection, and law enforcement. This cooperation ensures an integrated approach for protecting US forces; intelligence; national assets; US research, development, and technology; and the US economy. The Director of the DIA is the DOD functional manager for CI.

APPENDIX C: POLICY AND TACTICAL DOCTRINE RELATED TO INTELLIGENCE OPERATIONS

This section captures USAF policy documents and tactical doctrine that provide in-depth explanations related to intelligence operations. The policies outline the expectations for the AOC weapon system and Air Force forces (AFFOR) staff while also expanding on guidance to the USAF ISR enterprise about tradecraft and the exploitation of multiple intelligence disciplines. The tactical doctrine expands on the ISR roles in the AOC, the reachback capabilities of the DCGS enterprise, thoughts on ISR optimization, and the coordination between intelligence functions at the tactical and operational levels.

United States Air Force Policy	
AFI 13-103, *AFFOR Staff Operations, Readiness and Structures*, 19 November 2020	Provides guidance on an air component staff's organization, processes, and training to accomplish its function with the A2 portion described in Section 4.3.3., pp. 19 – 22.
AFI 13-1AOC, Volume 3, *Operational Procedures – AOC*, 18 December 2020	Describes all organizations, positions, and processes used by the AOC. While Chapter 6, *ISRD*, and Chapter 10, *Roles and Responsibilities*, outlines the duties for the bulk of specific intelligence teams and positions, the entire document should be reviewed for related material.
AFPD 14-4, *Management of the AF ISR & Cyber Effects Ops Enterprise*, 11 July 2019	Establishes USAF policy to ensure the Intelligence, Surveillance, Reconnaissance and Cyber Effects Operations Enterprise provides intelligence to theater customers and decision-makers at all levels while enabling the USAF to prepare for and conduct multi-domain operations throughout the competition continuum.
DAFMAN 14-401, *Intelligence Analysis & Targeting Tradecraft / Data Standards*, 26 May 2021	Implements AFPD 14-4 by defining USAF organizational responsibilities for intelligence analysis, targeting intelligence, and data standards in support of global integrated ISR and other service core functions, while ensuring consistency with the IC, DOD, and DAF doctrine, policy, and guidance.
AFMAN 14-405, *Multiple Source, Discipline, and Domain ISR*, 11 May 2020	Implements AFPD 14-4 by including guidance for conducting multi-source, multi-discipline ISR operations within the USAF ISR Enterprise. This manual lists the definitions, IC and DOD guidance, and organizational roles for the collection and exploitation of GEOINT, HUMINT, MASINT, OSINT, and SIGINT.
Air Force Intelligence Analysis Handbook, February 2018 (Common access card [CAC] required)	Formerly AFH 14-133, the HAF A2/6 Analysis directorate maintains this handbook to thoroughly describe how USAF intelligence analysis tradecraft is conducted to support IC, joint, and USAF missions.

United States Air Force Policy	
HAFMD 1-20, *Office of the Inspector General*, 05 Jan 2021	Explains the role of the Office of the Inspector General of the Department of the Air Force (SAF/IG), the administrative guidance and oversight of AFOSI, and the delegated authorities for CI.
AFMD 39, *Air Force Office of Special Investigations (AFOSI)*, 14 Apr 2020	Summarizes mission, organization, command structure, and delegations of authority from SecAF to the Commander, AFOSI.
AFI 71-101 Volume 4, *Counterintelligence*, 02 July 2019	Provides guidance for conducting CI activities and the programs and responsibilities of AFOSI.

United States Air Force Tactical Doctrine	
AFTTP 3-3.AOC, *Combat Fundamentals – Air Operations Center*, 23 October 2020 (CAC required)	Chapter 6, *Intelligence, Surveillance, and Reconnaissance*, describes the fundamental organization, roles, and responsibilities of the ISRD.
AFTTP 3-1.AOC, *Combat Fundamentals – Air Operations Center*, 23 October 2020 (on secure internet protocol router [SIPR])	Chapter 6, *Intelligence, Surveillance, and Reconnaissance*, expands on the organization, roles, and responsibilities of the ISRD at the classified level.
AFTTP 3-1.NTI, *National Tactical Integration*, 31 March 2017 (on JWICS)	Provides expanded descriptions of the ISRD's NTI team and the entire NTI enterprise at a classified level.
AFTTP 3-1.DCGS, *Distributed Common Ground Station*, 03 Dec 2021 (on SIPR)	Describes the reachback capabilities of the DCGS at the classified level.
AFTTP 3-1.DCGS, *Distributed Common Ground Station*, Annex 03 Dec 2021 (on JWICS)	Expands on specific DCGS capabilities at the classified level.
AFTTP 3-2.88, *ISR Optimization*, September 2019	Provides a comprehensive resource for planning, executing, and assessing surveillance, reconnaissance, and PED operations.

United States Air Force Tactical Doctrine	
AFTTP 3-3.IPE, *Integrated Planning & Employment*, 03 February 2022	Attachment 2, *Intelligence Support to Operations,* and Attachment 21, *Intelligence, Surveillance, and Reconnaissance*, provide the fundamental description of intelligence support to operations at the wing level and below, the intelligence coordination between the tactical and operational level, and a baseline description of the CIN.
AFTTP 3-1.IPE, *Integrated Planning & Employment*, 03 February 2022 (on SIPR)	Attachment 2, *Intelligence Support to Operations,* and Attachment 21, *Intelligence, Surveillance, and Reconnaissance*, expands on wing-level intelligence roles and functions at the classified level.
AFTTP 3-1.IPE, *Integrated Planning & Employment*, 03 February 2022 (on JWICS)	Attachment 2, *Intelligence Support to Operations,* and Attachment 21, *Intelligence, Surveillance, and Reconnaissance*, further expands on wing-level intelligence roles and functions at the classified level.
AFTTP 3-4.14, *Contingency Intelligence Network (CIN),* 15 December 2021 (on SIPR)	Describes the roles, missions, and responsibilities of the wing-level CIN in extensive detail at the classified level.
AFTTP 3-4.ABI, *Activity-Based Intelligence* (in DRAFT / CAC required)	Explains how ABI differs from traditional intelligence tradecraft and provides best practices and lessons learned for USAF Intelligence Airmen to support operations (in draft by ACC A2).

REFERENCES

All websites accessed 5 April 2023.

Doctrine can be accessed through links provided at: https://www.doctrine.af.mil/

US AIR FORCE DOCTRINE

https://www.doctrine.af.mil/

- AFDP 3-0, *Operations and Planning*
- AFDP 3-10, *Force Protection*
- AFDP 3-12, *Cyberspace Operations*
- AFDP 3-27, *Homeland Operations*
- AFDP 3-72, *Nuclear Operations*

JOINT DOCTRINE

Joint Electronic Library (JEL)

https://www.jcs.mil/Doctrine/

JEL +

https://jdeis.js.mil/jdeis/index.jsp?pindex=2

- JP 2-0, *Joint Intelligence*
- JP 3-60, *Joint Targeting*
- JP 5-0, *Joint Planning*
- *Joint Guide for Joint Intelligence Preparation of the Operational Environment*

TACTICAL DOCTRINE

Multi-Service Tactics Techniques and Procedures (MTTP):

https://www.alsa.mil/

- AFTTP 3-2.88, *MTTP for Intelligence, Surveillance, and Reconnaissance Optimization*

Air Force Weapon System TTP (AFTTP):

https://intelshare.intelink.gov/sites/561jts/SitePages/Home.aspx

- AFTTP 3-1.AOC, *Combat Fundamentals – Air Operations Center* (classified)
- AFTTP 3-1.DCGS, *Distributed Common Ground Station* (classified)
- AFTTP 3-1.IPE, *Integrated Planning & Employment* (classified)
- AFTTP 3-1.NTI, *National Tactical Integration* (classified)
- AFTTP 3-3.AOC, *Combat Fundamentals – Air Operations Center*
- AFTTP 3-3.IPE, *Integrated Planning & Employment*
- AFTTP 3-4.ABI, *Activity-Based Intelligence*

- AFTTP 3-4.14, *Contingency Intelligence Network* (classified)

MISCELLANEOUS PUBLICATIONS

- Air Force Instruction (AFI) 13-1AOC, Volume 3, *Operational Procedures – AOC*
- AFI 13-103, *AFFOR Staff Operations, Readiness and Structures*
- AFI 71-101, Volume 4, *Counterintelligence*
- *Air Force Intelligence Analysis Handbook*
- Air Force Manual (AFMAN) 11-202, Volume 3, *Flight Operations*
- AFMAN 14-405, *Multiple Source, Discipline, and Domain ISR*
- Air Force Mission Directive (AFMD) 39, *Air Force Office of Special Investigations*
- Air Force Policy Directive 14-4, *Management of the AF ISR & Cyber Effects Ops Enterprise*
- Department of the Air Force Manual 14-401, *Intelligence Analysis & Targeting Tradecraft / Data Standards*
- Headquarters Air Force Mission Directive 1-20, *Office of the Inspector General*