

FOR OFFICIAL USE ONLY

FM 2-0

INTELLIGENCE

HEADQUARTERS, DEPARTMENT OF THE ARMY

FINAL DRAFT

MARCH 2009

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

DESTRUCTION NOTICE—Destroy by any method that will prevent disclosure of contents or reconstruction of the document.

* This Publication Supersedes FM 2-0, 17 May 2004, with Change 1 dated 11 September 2008.

FOR OFFICIAL USE ONLY

2
Intelligence

3
Contents

	Page
4	
5	PREFACEv
6	INTRODUCTION.....vi
7	PART ONE INTELLIGENCE IN THE FULL SPECTRUM OPERATIONS
8	Chapter 1 INTELLIGENCE AND THE OPERATIONAL ENVIRONMENT..... 1-1
9	The Operational Environment 1-1
10	The Intelligence Warfighting Function 1-6
11	Purpose of Intelligence 1-7
12	Role of Intelligence 1-7
13	Intelligence Tasks..... 1-8
14	Characteristics of Effective Intelligence 1-18
15	Actionable Intelligence 1-19
16	The Intelligence Process 1-19
17	Continuing Activities 1-23
18	Army Intelligence Enterprise 1-27
19	Intelligence Disciplines 1-28
20	Emerging Capabilities 1-30
21	Chapter 2 INTELLIGENCE COMMUNITIES AND JOINT CONSIDERATIONS..... 2-1

DISTRIBUTION RESTRICTION: Distribution authorized to US. Government agencies only because it requires protection in accordance with AR 380-5 and as specified by DCS G-3 Message DTG 091913Z Mar 04. This determination was made on 12 January 2009. Contractor and other requests must be referred to ATTN: ATZS-CDI-D, US. Army Intelligence Center and Fort Huachuca, AZ 85613-7017, or via email at ATZS-FDC-D@conus.army.mil.

DESTRUCTION NOTICE—Destroy by any method that prevents disclosure of contents or reconstruction of the document in accordance with AR 380-5.

***This publication supersedes FM 2-0, 17 May 2004, with Change 1 dated 11 September 2008.**

FOR OFFICIAL USE ONLY

Contents

22	Intelligence Community.....	2-1
23	The Levels of War.....	2-5
24	Intelligence Reach.....	2-8
25	Categories of Intelligence Products.....	2-8
26	Unified Action Intelligence Operations.....	2-11
27	Force Projection Operations.....	2-17
28	PART TWO INTELLIGENCE IN FULL SPECTRUM OPERATIONS	
29	Chapter 3 FUNDAMENTALS IN FULL SPECTRUM OPERATIONS.....	3-1
30	The Operational Concept.....	3-1
31	Intelligence Support to the Elements of Full Spectrum Operations.....	3-2
32	Elements of Combat Power.....	3-4
33	Army Capabilities.....	3-5
34	Chapter 4 INTELLIGENCE PROCESS IN FULL SPECTRUM OPERATIONS.....	4-1
35	The Intelligence Process.....	4-1
36	PART THREE MILITARY INTELLIGENCE DISCIPLINES	
37	Chapter 5 ALL-SOURCE INTELLIGENCE.....	5-1
38	Definition.....	5-1
39	Role.....	5-2
40	Fundamentals.....	5-2
41	Planning.....	5-2
42	Operations.....	5-8
43	Chapter 6 COUNTERINTELLIGENCE.....	6-1
44	Definition.....	6-1
45	Mission.....	6-1
46	Role.....	6-1
47	Counterintelligence Functions.....	6-2
48	Counterintelligence Structure.....	6-6
49	Army Counterintelligence Levels of Employment.....	6-11
50	Joint Operations.....	6-16
51	Support to Contingency Operations.....	6-16
52	Support to Installations and Operating Bases.....	6-17
53	Operational Considerations.....	6-17
54	Counterintelligence Equipment.....	6-19
55	Chapter 7 HUMAN INTELLIGENCE.....	7-1
56	Human Intelligence-Related Definitions and Terms.....	7-1
57	Role of Human Intelligence.....	7-1
58	HUMINT Collection Methodologies.....	7-2
59	Capabilities and Planning Considerations.....	7-4
60	Human Intelligence Organizations.....	7-5
61	Human Intelligence Authorities.....	7-6
62	Human Intelligence Technical Channels.....	7-6
63	Chapter 8 GEOSPATIAL INTELLIGENCE.....	8-1

FOR OFFICIAL USE ONLY

64	Introduction.....	8-1
65	National System for Geospatial-Intelligence and National Geospatial-	
66	Intelligence Agency	8-1
67	Geospatial Intelligence within Army Doctrine.....	8-3
68	Chapter 9 IMAGERY INTELLIGENCE	9-1
69	Definition.....	9-1
70	Role	9-1
71	Fundamentals.....	9-1
72	Sources of Imagery	9-2
73	Types of Imagery Sensors	9-2
74	Imagery Intelligence in the Intelligence Process.....	9-3
75	Chapter 10 MEASUREMENT AND SIGNATURE INTELLIGENCE	10-1
76	Definition.....	10-1
77	Role	10-3
78	Fundamentals.....	10-3
79	Measurement and Signature Intelligence in the Intelligence Process	10-4
80	Chapter 11 OPEN-SOURCE INTELLIGENCE	11-1
81	Definition.....	11-1
82	Role of Open-Source Intelligence	11-1
83	Fundamentals of Open-Source Information	11-2
84	Open-Source Intelligence Considerations.....	11-2
85	Open-Source Media	11-6
86	Chapter 12 SIGNALS INTELLIGENCE	12-1
87	Definition.....	12-1
88	Role	12-1
89	Fundamentals.....	12-1
90	Signals Intelligence in the Intelligence Process	12-3
91	Chapter 13 TECHNICAL INTELLIGENCE	13-1
92	Definition.....	13-1
93	Role	13-1
94	Fundamentals.....	13-2
95	Technical Intelligence in the Intelligence Process	13-4
96	Appendix A EXAMPLE INTELLIGENCE SUMMARY, INTELLIGENCE ESTIMATE, AND	
97	INTELLIGENCE RUNNING ESTIMATE FORMATS	A-1
98	Appendix B LANGUAGE SUPPORT	B-17
99	GLOSSARY	Glossary-1
100	REFERENCES	References-1
101	INDEX.....	Index-1
102		

103

Figures

FOR OFFICIAL USE ONLY

Contents

104	Figure 1-1. The intelligence process.....	1-20
105	Figure 1-2. Example of the tactical portion of the Army intelligence enterprise	1-28
106	Figure 2-1. Intelligence community membership	2-2
107	Figure 2-2. Levels of war	2-6
108	Figure 2-3. Notional joint task force J-2 organization	2-14
109	Figure 2-4. Typical joint intelligence support element	2-16
110	Figure 4-1. The operations process	4-1
111	Figure 4-2. The relationship between the operations and intelligence processes	4-2
112	Figure 4-3. Requirements development and integration into the ISR process.....	4-6
113	Figure 6-1. 2X organization.....	6-7
114	Figure A-1. Example INTSUM format	A-2
115	Figure A-2. Example format of an intelligence estimate	A-3
116	Figure A-3. Example of an intelligence running estimate format.....	A-8
117		

Tables

118		
119	Table 1-1. Intelligence tailored to the commander's needs.....	1-9
120	Table 2-1. Examples of partners and sources for intelligence reach	2-9
121	Table 3-2. Army command relationships and inherent responsibilities	3-7
122	Table 4-1. Presentation methods and products.....	4-15
123	Table 9-1. Sensor characteristics matrix	9-3
124	Table 11-1. Open-source intelligence classification considerations.....	11-4
125	Table 11-2. Primary open-source media	11-7
126	Table B-1. Special staff officer responsibilities	B-22
127	Table B-2. Personal staff officer responsibilities.....	B-23
128		
129		

FOR OFFICIAL USE ONLY

Preface

130

131 FM 2-0 is the Army's keystone manual for military intelligence (MI) doctrine. It describes—

- 132 • The fundamentals of intelligence operations.
- 133 • The operational environment.
- 134 • The intelligence warfighting function.
- 135 • The intelligence process.
- 136 • MI roles and functions within the context of Army operations.
- 137 • Intelligence in unified action.
- 138 • Intelligence considerations in strategic readiness.
- 139 • The intelligence disciplines.

140 The significant intelligence updates and changes in this manual from FM 2-0,
141 17 May 2004, with Change 1 dated 11 September 2008, are detailed in the Introduction. This manual conforms
142 to the overarching doctrinal precepts presented in FM 3-0.

143 This FM provides doctrinal guidance for the intelligence warfighting function in support of commanders and
144 staffs. It also serves as a reference for personnel who are developing doctrine; tactics, techniques, and
145 procedures (TTP); materiel and force structure; and institutional and unit training for intelligence operations.

146 This FM provides MI guidance for commanders, staffs, trainers, and MI personnel at all echelons. It forms the
147 foundation for MI and intelligence warfighting function doctrine development.

148 This FM applies to the Active Army, the Army National Guard (ARNG)/Army National Guard of the United
149 States (ARNGUS), and the United States Army Reserve (USAR). It is also intended for commanders and staffs
150 of joint and combined commands, US Naval and Marine Forces, units of the US Air Force, and the military
151 forces of multinational partners.

152 Headquarters, US Army Training and Doctrine Command, is the proponent for this publication. The preparing
153 agency is the US Army Intelligence Center and School. Send written comments and recommendations on
154 DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to Commander, ATZS-
155 FDT- (FM 2-0), 550 Cibique Street, Fort Huachuca, AZ 85613-7017. Send comments and recommendations by
156 email to ATZS-FDC-D@conus.army.mil. Follow the DA Form 2028 format or submit an electronic DA Form
157 2028.

158

FOR OFFICIAL USE ONLY

159

Introduction

160 FM 2-0 updates the Army's keystone doctrine on intelligence. The following paragraphs summarize the
161 most important updates and changes from FM 2-0, 17 May 2004, with change 1 dated 11 September 2008.

162 **Chapter 1** makes the following changes:

- 163 • Replaces the intelligence battlefield operating system with the intelligence warfighting function
164 and discusses the mission variables for which the intelligence warfighting function is
165 responsible: enemy, terrain (to include weather), and civil considerations.
- 166 • Updates the intelligence tasks (METL).
- 167 • Addresses the concept of actionable intelligence.
- 168 • Describes the Characteristics of Effective Intelligence which includes the six relevant
169 information quality criteria plus three additional criteria.
- 170 • Updates the definition of priority intelligence requirements and describes intelligence
171 requirements.
- 172 • Updates the intelligence process, adding a step (Generate Intelligence Knowledge), combining
173 the Collect and Process steps, changing the Disseminate continuing activity to Propagate and
174 describing and additional input to the intelligence process (Commander's Input).
- 175 • Introduces the concept of the intelligence survey as a means to provide the unit intelligence
176 officer with an initial assessment for recommending intelligence asset apportionment within the
177 area of operation (AO) and how best to use the unit's intelligence assets within the AO.
- 178 • Addresses the concept of critical thinking.
- 179 • Increases the number of intelligence disciplines from seven to nine by adding geospatial
180 intelligence (GEOINT) and open-source intelligence (OSINT).

181 **Chapter 2** makes the following changes:

- 182 • Updates Joint Intelligence Organizations based on JP 2-0 and JP 3-33.
- 183 • Updates Unified Action and Force Projection Operations sections based on FM 3-0.
- 184 • Discusses the concept and includes the Army definition of reconnaissance, surveillance, and
185 target acquisition/intelligence, surveillance, and reconnaissance (RSTA/ISR).

186 **Chapter 3** updates the operational concept, operations definitions, and Army capabilities and introduces
187 the elements of combat power based on FM 3-0.

188 **Chapter 4** makes the following changes:

- 189 • Further addresses the Generate Knowledge step during the intelligence and operations process
190 interaction.
- 191 • Addresses the concept of Red Teaming.

192 **Chapters 5 through 13** make the following changes:

- 193 • Incorporates the updated steps of the IPB process in accordance with FM 2-01.3.
- 194 • Updates the counterintelligence functions and organizations.
- 195 • Updates human intelligence (HUMINT) functions and organizations based on FM 2-22.3.
- 196 • Introduces GEOINT as an intelligence discipline and discusses the Army implementation of
197 GEOINT.

FOR OFFICIAL USE ONLY

-
- 198
- 199
- 200
- 201
- 202
- 203
- 204
- 205
- 206
- Updates the imagery intelligence (IMINT) definitions.
 - Incorporates changes to the measurement and signature intelligence (MASINT) discipline.
 - Introduces OSINT as an intelligence discipline.
 - Updates signals intelligence (SIGINT) definitions and organizations.
 - Provides an example format for the intelligence summary, intelligence estimate and the intelligence running estimate.
 - Updates the linguist support section.
 - Adds a short discussion of language technology.

FOR OFFICIAL USE ONLY

207

PART ONE

208

Intelligence in the Full Spectrum Operations

209
210
211
212

Part One discusses the role of intelligence from stable peace to general war and back to stable peace. The primary focus of the intelligence warfighting function is to provide timely, relevant, accurate, predictive, and tailored intelligence that focuses missions and operations in the right places at the right time.

213
214
215
216
217
218

Chapter 1 describes the operational environment and the roles of intelligence within the operational environment. It introduces the intelligence warfighting function, the intelligence tasks, and the intelligence process, which are the mechanisms through which the intelligence warfighting function supports the warfighter. This chapter also introduces the intelligence disciplines, which are explained in detail in Part Three of this manual.

219
220
221
222
223

Chapter 2 describes the interaction of the intelligence warfighting function within the nation's intelligence community structure; it provides an overview of the intelligence community at the national level and the unified action level—joint, interagency, intergovernmental, and multinational (JIIM) and aspects of full spectrum operations. This chapter also discusses the concepts and components of intelligence reach.

224

Chapter 1

225

Intelligence and the Operational Environment

226

THE OPERATIONAL ENVIRONMENT

227
228
229
230

1-1. **The operational environment is a composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decision of the commander (JP 3-0).** The operational environment encompasses physical areas and factors of the air, land, maritime, and space domains. It also includes the information environment and enemy, adversary, friendly, and neutral systems.

231

OPERATIONAL VARIABLES

232
233
234
235
236
237

1-2. Analysis of the operational environment—in terms of political, military, economic, social, information, infrastructure, with the addition of physical environment and time (PMESII-PT) variables—provides relevant information that senior commanders use to understand, visualize, and describe the operational environment. As a set, these operational variables are often abbreviated as PMESII-PT.

FOR OFFICIAL USE ONLY

238 **Political**

239 1-3. The political variable describes the distribution of responsibility and power at all levels of
240 governance.

241 1-4. Political structures and processes enjoy varying degrees of legitimacy with populations from the
242 local through international levels. Formally constituted authorities and informal or covert political powers
243 strongly influence events. Political leaders can use ideas, beliefs, actions, and violence to enhance their
244 power and control over people, territory, and resources. Many sources of political motivation exist. These
245 may include charismatic leadership; indigenous security institutions; and religious, ethnic, or economic
246 communities. Political opposition groups or parties also affect the situation. Each may deal differently with
247 US or multinational forces. Understanding the political circumstances helps commanders and staffs
248 recognize key organizations and determine their aims and capabilities.

249 1-5. Understanding political implications requires analyzing all relevant partnerships—political,
250 economic, military, religious, and cultural. This analysis captures the presence and significance of external
251 organizations and other groups; these include groups united by a common cause. Examples are private
252 security organizations, transnational corporations, and nongovernmental organizations (NGOs) that
253 provide humanitarian assistance.

254 1-6. A political analysis also addresses the effect of will. Will is the primary intangible factor; it
255 motivates participants to sacrifice to persevere against obstacles. Understanding the motivations of key
256 groups (for example, political, military, and insurgent) helps clarify their goals and willingness to sacrifice
257 to achieve their ends.

258 1-7. The political variable includes the US domestic political environment. Therefore, mission analysis
259 and monitoring the situation includes an awareness of national policy and strategy.

260 **Military**

261 1-8. The military variable includes the military capabilities of all armed forces in a given operational
262 environment. For many states, an army is the military force primarily responsible for maintaining internal
263 and external security. Paramilitary organizations and guerrilla forces may influence friendly and hostile
264 military forces. Militaries of other states not directly involved in a conflict may also affect them. Therefore,
265 analysis should include the relationship of regional land forces to the other variables. Military analysis
266 examines the capabilities of enemy, adversary, host nation (HN), and multinational military organizations.
267 Such capabilities include—

- 268 ● Equipment.
- 269 ● Manpower.
- 270 ● Doctrine.
- 271 ● Training levels.
- 272 ● Resource constraints.
- 273 ● Leadership.
- 274 ● Organizational culture.
- 275 ● History.
- 276 ● Nature of civil-military relations.

277 1-9. Understanding these factors helps commanders estimate the actual capabilities of each armed force.
278 Analysis should focus on each organization's ability to field capabilities and use them domestically,
279 regionally, and globally.

280

FOR OFFICIAL USE ONLY

281 **Economic**

282 1-10. The economic variable encompasses individual and group behaviors related to producing,
 283 distributing, and consuming resources. Specific factors may include the influence of—

- 284 ● Industrial organizations.
- 285 ● Trade.
- 286 ● Development (including foreign aid).
- 287 ● Finance.
- 288 ● Monetary policy and conditions.
- 289 ● Institutional capabilities.
- 290 ● Geography.
- 291 ● Legal constraints (or the lack of them) on the economy.

292 1-11. While the world economy is becoming interdependent, local economies differ. These differences
 293 significantly influence political choices, including individuals' decisions to support or subvert the existing
 294 order. Many factors create incentives or disincentives for individuals and groups to change the economic
 295 status quo. These may include—

- 296 ● Technical knowledge.
- 297 ● Decentralized capital flows.
- 298 ● Investment.
- 299 ● Price fluctuations.
- 300 ● Debt.
- 301 ● Financial instruments.
- 302 ● Protection of property rights.
- 303 ● Existence of black market or underground economies.

304 1-12. Thus, indicators measuring potential benefits or costs of changing the political-economic order may
 305 enhance understanding the social and behavioral dynamics of friendly, adversary, and neutral entities.

306 **Social**

307 1-13. The social variable describes societies within an operational environment. A society is a population
 308 whose members are subject to the same political authority, occupy a common territory, have a common
 309 culture, and share a sense of identity. Societies are not monolithic. They include diverse social structures.
 310 Social structure refers to the relations among groups of persons within a system of groups. It includes
 311 institutions, organizations, networks, and similar groups. (FM 3-24 discusses socio-cultural factors analysis
 312 and social network analysis.)

313 1-14. Culture comprises shared beliefs, values, customs, behaviors, and artifacts that society members use
 314 to cope with their world and with one another. Societies usually have a dominant culture but may have
 315 many secondary cultures. Different societies may share similar cultures, but societal attributes change over
 316 time. Changes may occur in any of the following areas:

- 317 ● Demographics.
- 318 ● Religion.
- 319 ● Migration trends.
- 320 ● Urbanization.
- 321 ● Standards of living.
- 322 ● Literacy and nature of education.
- 323 ● Cohesiveness and activity of cultural, religious, or ethnic groups.

FOR OFFICIAL USE ONLY

324 1-15. Social networks, social status and related norms, and roles that support and enable individuals and
325 leaders require analysis. This analysis should also address societies outside the operational area whose
326 actions, opinions, or political influence can affect the mission.

327 1-16. People base their actions on perceptions, assumptions, customs, and values. Cultural awareness helps
328 identify points of friction within populations, helps build rapport, and reduces misunderstandings. It can
329 improve a force's ability to accomplish its mission and provide insight into individual and group intentions.
330 However, cultural awareness requires training before deploying to an unfamiliar operational environment
331 and continuous updating while deployed. Commanders develop their knowledge of the societal aspects
332 within their areas of operations (AO) to a higher level of cultural astuteness, one that allows them to
333 understand the impact of their operations on the population and prepares them to meet local leaders face-
334 to-face.

335 **Information**

336 1-17. Joint doctrine defines the *information environment* as the aggregate of individuals, organizations,
337 and systems that collect, process, disseminate, or act on information (JP 3-13). The environment shaped by
338 information includes leaders, decision makers, individuals, and organizations. The global community's
339 access and use of data, media, and knowledge systems occurs in the information shaped by the operational
340 environment. Commanders use information engagement to shape the operational environment as part of
341 their operations.

342 1-18. Media representatives significantly influence the information that shapes the operational
343 environment. Broadcast and Internet media sources can rapidly disseminate competing views of military
344 operations worldwide. Adversaries often seek to further their aims by controlling and manipulating how
345 audiences at all levels perceive a situation's content and context. Media coverage influences US political
346 decision making, popular opinion, and multinational sensitivities.

347 1-19. Complex telecommunications networks now provide much of the globe with a vast web of
348 communications capabilities. Observers and adversaries have unprecedented access to multiple information
349 sources. They often attempt to influence opinion by providing their own interpretation of events. Televised
350 news and propaganda reach many people. However, in developing countries, information still may flow by
351 less sophisticated means such as messengers and graffiti. Understanding the various means of
352 communications is important. Observers and adversaries control information flow and influence audiences
353 at all levels.

354 **Infrastructure**

355 1-20. Infrastructure comprises the basic facilities, services, and installations needed for a society's
356 functioning. Degrading infrastructure affects the entire operational environment. Infrastructure also
357 includes technological sophistication—the ability to conduct research and development and apply the
358 results to civil and military purposes.

359 1-21. Not all segments of society view infrastructure in the same way. Improvements viewed by some as
360 beneficial may not be perceived as such by all. One community may perceive certain improvements as
361 favoring other communities at its expense. Effective information engagement is necessary to address such
362 concerns. Actions affecting infrastructure require a thorough analysis of possible effects.

363 **Physical Environment**

364 1-22. The physical environment includes the geography and manmade structures in the operational area.
365 The following factors affect the physical environment:

- 366 ● Manmade structures, particularly urban areas.
- 367 ● Climate and weather.
- 368 ● Topography.

FOR OFFICIAL USE ONLY

- 369 ● Hydrology.
- 370 ● Natural resources.
- 371 ● Biological features and hazards.
- 372 ● Other environmental conditions.

373 1-23. The enemy understands that less complex and open terrain often exposes their military weaknesses.
 374 Therefore, they may try to counteract US military advantages by operating in urban or other complex
 375 terrain and during adverse weather conditions.

376 Time

377 1-24. Time is a significant consideration in military operations. Analyzing it as an operational variable
 378 focuses on how an operation's duration might help or hinder each side. This has implications at every
 379 planning level. An enemy with limited military capability usually views protracted conflict as
 380 advantageous to them. They avoid battles and only engage when conditions are overwhelmingly in their
 381 favor. This is a strategy of exhaustion. Such a strategy dominated the American Revolution and remains
 382 effective today. The enemy concentrates on surviving and inflicting friendly and civilian casualties over
 383 time. Although the military balance may not change, this creates opportunities to affect the way domestic
 384 and international audiences view the conflict. Conversely, a hostile power may attempt to mass effects and
 385 achieve decisive results in a short period.

386 1-25. While the operational variables are directly relevant to campaign planning, they may be too broad to
 387 be applied directly to tactical planning. That does not mean they are not of value at all levels; they are
 388 fundamental to developing the understanding of the operational environment necessary to conduct planning
 389 at any level, in any situation.

390 1-26. When identifying threats based on the systems approach to PMESII, there are three primary
 391 components of the operational environment for which the intelligence warfighting function is responsible:
 392 threat, terrain (to include the weather), and civil considerations.

393 1-27. The degree to which each operational variable provides useful information depends on the situation
 394 and echelon. Once the G-2/S-2 has completed their overall analysis, they must go back and factor in small
 395 unit leaders' intelligence requirements. For example, social and economic variables often receive close
 396 analysis as part of enemy and civil considerations at brigade and higher levels. They may affect the training
 397 and preparation of small units. However, they may not be relevant to a small-unit leader's mission analysis.
 398 That leader may only be concerned with questions, such as "Who is the tribal leader for this village?" "Is
 399 the electrical generator working?" "Does the enemy have antitank missiles?"

400 MISSION VARIABLES

401 1-28. Upon receipt of a warning order (WARNO) or mission, Army leaders narrow their focus to six
 402 mission variables. Mission variables are those aspects of the operational environment that directly affect a
 403 mission. They outline the situation as it applies to a specific Army unit. The mission variables are mission,
 404 enemy, terrain and weather, troops and support available, time available, and civil considerations
 405 (METT-TC). These are the categories of relevant information used for mission analysis. Army leaders use
 406 the mission variables to synthesize operational variables and tactical-level information with local
 407 knowledge about conditions relevant to their mission. The intelligence warfighting function is responsible
 408 for describing the enemy, terrain and weather, and civil considerations:

- 409 ● **Enemy.** Relevant information regarding the enemy may include the following:
 - 410 ■ Threat characteristics (previously order of battle factors).
 - 411 ■ Threat courses of action (COAs).
- 412 ● **Terrain and Weather.** Terrain and weather are natural conditions that profoundly influence
 413 operations. Terrain and weather are neutral; they favor neither side unless one is more familiar
 414 with—or better prepared to operate in—the environment.

FOR OFFICIAL USE ONLY

- 415 ● **Civil Considerations.** Civil considerations comprise six characteristics expressed in the
416 memory aid ASCOPE:
417 ■ Areas.
418 ■ Structures.
419 ■ Capabilities.
420 ■ Organizations.
421 ■ People.
422 ■ Events.

423 *Note.* For additional information on ASCOPE and the intelligence preparation of the battlefield
424 (IPB) process, see FM 2-01.3. Understanding the operational environment requires
425 understanding the civil aspects of the area of influence. Civil considerations reflect how the
426 manmade infrastructure, civilian institutions, and the attitudes and activities of the civilian
427 leaders, populations, and organizations within an AO influence the conduct of military
428 operations.

429 1-29. METT-TC enables leaders to synthesize operational level information with local knowledge relevant
430 to their missions and tasks in a specified AO. Tactical and operational leaders can then anticipate the
431 consequences of their operations before and during execution. See FM 3-0 for a detailed discussion of
432 PMESII-PT and METT-TC.

433 THE INTELLIGENCE WARFIGHTING FUNCTION

434 1-30. *The intelligence warfighting function is the related tasks and systems that facilitate understanding of*
435 *the operational environment, enemy, terrain, and civil considerations (FM 3-0). It includes tasks*
436 *associated with intelligence, surveillance, and reconnaissance (ISR) operations and is driven by the*
437 *commander. Intelligence is more than just collection. It is a continuous process that involves analyzing*
438 *information from all sources and conducting operations to develop the situation. The intelligence*
439 *warfighting function includes the following tasks:*

- 440 ● Support to force generation.
441 ● Support to situational understanding.
442 ● Perform ISR.
443 ● Support to targeting and information superiority.

444 1-31. The intelligence warfighting function is one of six warfighting functions—movement and maneuver,
445 intelligence, fires, sustainment, command and control (C2), and protection. *A warfighting function is a*
446 *group of tasks and systems (people, organizations, information, and processes) united by a common*
447 *purpose that commanders use to accomplish missions and training objectives (FM 3-0). (See FM 3-0,*
448 *chapter 4, for a detailed discussion of the warfighting functions.) The intelligence warfighting function is a*
449 *flexible force of personnel, organizations, and equipment that, individually or collectively, provide*
450 *commanders with the timely, relevant, accurate, predictive, and tailored intelligence required to visualize*
451 *the AO, assess the situation, and direct military actions. Additionally, the intelligence warfighting*
452 *function—*

- 453 ● Is a complex system that operates worldwide, from below ground to space, in support of an
454 operation, to include the ability to leverage theater and national capabilities.
455 ● Requires cooperation and division of ISR and analysis efforts internally, higher, lower, adjacent,
456 and across components and multinational forces.

457 1-32. The intelligence warfighting function not only includes assets within the MI branch but also includes
458 the assets of all branches or warfighting functions that conduct intelligence warfighting function tasks.
459 Every Soldier, as a part of a small unit, is a potential information collector and an essential component to

FOR OFFICIAL USE ONLY

460 help reach situational understanding. Each Soldier develops a special level of awareness simply due to
461 exposure to events occurring in the AO and has the opportunity to collect and report information by
462 observation and interaction with the population (see paragraph 3-3).

463 1-33. Planning and executing military operations will require intelligence regarding the threat (traditional,
464 irregular, catastrophic, and disruptive) and the AO. The intelligence warfighting function generates
465 intelligence and intelligence products that portray the enemy and aspects of the environment. These
466 intelligence products enable the commander to identify potential COAs, plan operations, employ forces
467 effectively, employ effective tactics and techniques, and implement protection.

468 1-34. The intelligence warfighting function is always engaged in supporting the commander in offensive,
469 defensive, stability, and, when directed, civil support operations. Intelligence provides products that are
470 timely, relevant, accurate, predictive, and tailored. Hard training, thorough planning, meticulous
471 preparation, and aggressive execution posture the Army for success. In the current environment we must
472 maintain intelligence readiness to support operations. This support reaches across full spectrum operations
473 and levels of war to produce the intelligence required to successfully accomplish the mission through a
474 combination of space, aerial, seaborne, and ground-based systems to provide the most comprehensive
475 intelligence possible. During force projection operations, the intelligence warfighting function supports the
476 commander with accurate and responsive intelligence from predeployment through redeployment.

477 1-35. The intelligence warfighting function architecture provides specific intelligence and communications
478 structures at each echelon from the national level through the tactical level. (In recent years, brigade
479 combat team [BCT] intelligence capabilities and access have been significantly increased.) These structures
480 include intelligence organizations, systems, and procedures for generating intelligence knowledge,
481 planning, preparing, collecting, and producing intelligence and other critical information in a useable form
482 to those who need it, when they need it. Effective communications connectivity and automation are
483 essential components of this architecture.

484 **PURPOSE OF INTELLIGENCE**

485 1-36. The purpose of intelligence is to provide commanders and their staffs with timely, relevant, accurate,
486 predictive, and tailored intelligence about the enemy and the environment in a timely manner. Intelligence
487 supports the planning, preparing, execution, and assessment of missions. The most important role of
488 intelligence is to support the commander's decision making to drive operations. Intelligence must be
489 timely, relevant, accurate, predictive, and tailored.

490 **ROLE OF INTELLIGENCE**

491 1-37. Intelligence drives the conduct of operations; therefore, the G-2/S-2 is responsible for ensuring that
492 the intelligence warfighting function operates smoothly and efficiently so that the commander receives
493 timely, relevant, accurate, predictive, and tailored information in a timely manner. The G-2/S-2 is not
494 simply a manager but is the primary advisor to the commander on how to utilize ISR assets, supports the
495 commander with analysis and production, and drives ISR collection.

496 1-38. The commander requires intelligence about the enemy and the environment prior to engaging in
497 operations in order to effectively execute battles, engagements, and other missions within full spectrum
498 operations. Intelligence assists the commander in visualizing the environment, organizing the forces, and
499 controlling operations to achieve the desired objectives or end-state. Intelligence supports protection by
500 alerting the commander to threats and assisting in preserving and protecting the force.

501 1-39. The unit may need to deal with multiple threats. The commander must understand how current and
502 potential enemies organize, equip, train, employ, and control their forces. Intelligence provides an
503 understanding of the enemy, which assists in planning, preparing, executing, and assessing military
504 operations. The commander must also understand the AO and area of influence and their effects on both
505 friendly and threat operations. The commander receives mission-oriented intelligence on enemy forces and

FOR OFFICIAL USE ONLY

506 the AO and area of influence from the G-2/S-2. The G-2/S-2 depends upon the ISR effort to collect and
507 provide information on the threat and environment.

508 1-40. One of the most significant contributions that intelligence personnel can accomplish is to accurately
509 predict possible enemy events and actions. Although intelligence is never perfect and can be extremely
510 time consuming and difficult, providing worst case and probable COA based on verified or probable threat
511 capability and intent during wargaming is a core intelligence function. Thus, predictive intelligence enables
512 the commander and staff to anticipate key enemy events or reactions and develop corresponding plans or
513 counteractions. Intelligence professionals must tailor the intelligence to the commander's requirements to
514 support the commander's situational understanding. Commanders must receive the intelligence in a format
515 that is clear and concise so they can understand it, believe it, and act on it. It is the G-2/S-2's primary
516 function to deliver that intelligence to the commander in a timely manner. In order for intelligence
517 professionals to provide the best possible support and to tailor products to the commanders' needs, the
518 commander and the G-2/S-2 must develop a close professional relationship. Through this doctrinal
519 concept, intelligence drives operations.

520 INTELLIGENCE TASKS

521 1-41. The personnel and organizations within the intelligence warfighting function conduct four primary
522 intelligence tasks that facilitate the commander's visualization and understanding of the threat and the
523 environment. These tasks are interactive and often take place simultaneously. (Refer to FM 7-15 for the
524 complete subordinate task listing.) Table 1-1 shows these tasks tailored to the commander's needs.

525 SUPPORT TO FORCE GENERATION

526 1-42. Support to force generation is the task of generating knowledge concerning an area of possible
527 employment or deployment, facilitating future intelligence operations, and tailoring the force. It includes
528 establishing intelligence communication architecture and developing the intelligence staff's knowledge
529 management—these enable intelligence reach, collaborative analysis, data storage, processing, and analysis
530 and intelligence production between the strategic and operational intelligence communities to the tactical
531 intelligence warfighting function. This task consists of five subtasks.

532 Provide Intelligence Readiness

533 1-43. Intelligence readiness operations support ongoing operations, contingency planning, and operational
534 preparation by developing baseline knowledge of multiple potential threats and operational environments.
535 These operations and related intelligence training activities enable the intelligence warfighting function to
536 support the commander's intelligence requirements effectively. This task consists of three subtasks:

- 537 ● **Perform Indications & Warnings (I&W).** This activity provides the commander with advance
538 warning of threat actions or intentions. The intelligence officer develops I&W to alert the
539 commander rapidly of events or activities that would change the basic nature of the operations.
540 I&W enables the commander to quickly reorient the force to unexpected contingencies and
541 shape the operational environment.
- 542 ● **Conduct Intelligence Readiness Operations.** Intelligence readiness operations support
543 contingency planning and preparation by developing baseline knowledge of multiple potential
544 threats and operational environments. This information and training enables a collaborative
545 effort and environment to provide the best possible initial threat understanding.
- 546 ● **Conduct Foundry.** Foundry is a training program designed to sustain critical intelligence
547 capabilities, perishable intelligence skills, and provide regional focus, technical training, and
548 functional expertise for the tactical MI force through home-station training platforms, mobile
549 training teams, and live environment training opportunities. Foundry provides a single "hub" for
550 advanced skills training across the Active Army, ARNG, and USAR MI force, as well as train
551 leaders who supervise MI missions and all Soldiers who perform MI activities.

FOR OFFICIAL USE ONLY

Table 1-1. Intelligence tailored to the commander's needs

Intelligence Tasks ▶	Commander's Focus ▶	Commander's Decisions
<p>Support to Force Generation</p> <ul style="list-style-type: none"> • Provide Intelligence Readiness. • Establish Intelligence Architecture. • Provide Intelligence Overwatch. • Generate Intelligence. • Tailor the Intelligence Force. 	<p>Orient on contingencies.</p>	<p>Should the unit's level of readiness be increased?</p> <p>Should the OPLAN be implemented?</p>
<p>Support to Situational Understanding</p> <ul style="list-style-type: none"> • Perform Intelligence Preparation of the Battlefield. • Perform Situation Development. • Provide Intelligence Support to Protection. • Provide Tactical Intelligence Overwatch. • Conduct Police Intelligence Operations. 	<p>Plan an operation. Prepare. Execute. Assess. Secure the force.</p>	<p>Which COA will I implement?</p> <p>Which enemy actions are expected?</p>
<p>Perform Intelligence, Surveillance, and Reconnaissance</p> <ul style="list-style-type: none"> • Perform ISR Synchronization. • Perform ISR Integration. • Conduct Reconnaissance. • Conduct Surveillance. • Conduct Related Missions and Operations. 	<p>Plan an operation. Prepare. Execute. Assess.</p>	<p>Which DPs, HPTs, HVTs, are linked to the enemy's actions?</p> <p>Are the assets available and in position to collect on the DPs, HPTs, HVTs?</p> <p>Have the assets been repositioned for contingency missions?</p>
<p>Support to Targeting and Information Superiority</p> <ul style="list-style-type: none"> • Provide Intelligence Support to Targeting. • Provide Intelligence Support to Information Superiority. • Provide Intelligence Support to Combat Assessment. 	<p>Utilize lethal or nonlethal fires against targets.</p> <p>Destroy/suppress/neutralize targets.</p> <p>Reposition intelligence or attack assets.</p>	<p>Is the unit's fire (lethal and nonlethal) and maneuver effective?</p> <p>Should the same targets be reengaged?</p> <p>Is the unit's information engagement effective?</p>

552 **Establish Intelligence Architecture**

553 1-44. Intelligence architecture activity includes complex and technical issues like sensors, dataflow,
554 hardware, software, communications, communications security (COMSEC) materials, network

FOR OFFICIAL USE ONLY

555 classification, technicians, database access, liaison officers (LNOs), training, and funding. Well-defined
556 and designed intelligence architecture can offset or mitigate structural, organizational, or personnel
557 limitations. This architecture provides the best possible threat, terrain, weather, and civil considerations
558 understanding. This task consists of four subtasks:

- 559 ● **Conduct Intelligence Reach.** *Intelligence reach is a process by which intelligence*
560 *organizations proactively and rapidly access information from, receive support from, and*
561 *conduct direct collaboration and information sharing with other units and agencies both*
562 *deployed in theater and outside the theater unconstrained by geographic proximity, echelon, or*
563 *command (TC 2-33.5). Such intelligence helps prepare for the mission and answer the*
564 *commander's critical information requirements (CCIRs) during the mission directly from the*
565 *source (pull) without the need to wait for the information to come to them (push).*
- 566 ● **Develop and Maintain Automated Intelligence Networks.** Use existing automated
567 information systems, such as the Distributed Common Ground System-Army (DCGS-A), or
568 create operationally specific networks to connect unique assets, units, echelons, agencies, or
569 multinational partners for intelligence, collaborative analysis and production, dissemination, and
570 intelligence reach. These networks include accessibility and interoperability across the AO, to
571 include unclassified and classified means. This task includes identifying deficiencies in systems
572 or networks, Service procedures, system administration procedures, security procedures,
573 alternate power plan, redundancy capability, system backups, and update procedures.
- 574 ● **Establish and Maintain Access.** Establish and provide access to classified and unclassified
575 programs, databases, networks, systems, and other web-based collaborative environments for
576 Army, joint, interagency, and multinational organizations to facilitate intelligence reporting,
577 production, dissemination, sustainment, intelligence reach, and a multi-level collaborative
578 information environment.
- 579 ● **Create and Maintain Intelligence Databases.** Create and maintain unclassified and classified
580 databases to create interoperable and collaborative environments for Army, joint, interagency,
581 and multinational organizations to facilitate intelligence analysis, reporting, production,
582 dissemination, sustainment, and intelligence reach. This subtask also includes the requirements
583 for format and standardization, indexing and correlation, normalization, storage, security
584 protocols, and associated applications. The following must be addressed in database
585 development, management, and maintenance:
 - 586 ■ Data sources.
 - 587 ■ Information redundancy.
 - 588 ■ Import and export standards.
 - 589 ■ Data management.
 - 590 ■ Update and backup procedures.
 - 591 ■ Data mining, query, and search protocols.

592 **Provide Intelligence Overwatch**

593 1-45. Intelligence overwatch is creating standing, fixed analytical intelligence capabilities that provide
594 dedicated intelligence support and overwatch to committed maneuver units. The overwatch cell is
595 connected via a shared intelligence network that can pull information from multiple sources and provide
596 succinct answers (vice megabytes of information) directly to supported units when time is of the essence.

597 **Generate Intelligence Knowledge**

598 1-46. Generate intelligence knowledge is a continuous and user-defined task driven by the commander that
599 begins prior to mission receipt and provides the relevant knowledge required concerning the operational
600 environment for the conduct of operations. Generate intelligence knowledge uses these components as a
601 start point to acquire and organize the information. The execution of this task must follow all applicable
602 policies and regulations on the collection of information and operations security (OPSEC). The information

FOR OFFICIAL USE ONLY

603 and intelligence obtained are refined for use in mission analysis through functional analysis. Knowledge is
 604 obtained through intelligence reach; research; data mining; database access; academic studies, products, or
 605 materials; intelligence archives; OSINT; or other information sources that support the conduct of
 606 operations. The execution of this task must follow all applicable policies and regulations on the collection
 607 of information and OPSEC. This task contains five subtasks:

- 608 • **Develop the Foundation to Define Threat Characteristics.** Obtain detailed information and
 609 intelligence concerning threat characteristics affecting the conduct of operations. Obtain this
 610 information through intelligence reach; research; data mining; database access; academic
 611 studies, products, or materials; intelligence archives; OSINT; or other information sources to
 612 support operations, planning, execution, and commander's decisions. This subtask requires
 613 specific and detailed information for each threat characteristic.
- 614 • **Obtain Detailed Terrain Information and Intelligence.** Obtain detailed information and
 615 intelligence on the terrain of the expected area of interest (AOI) through intelligence reach;
 616 research; data mining; database access; academic studies, products, or materials; intelligence
 617 archives; OSINT; or other information sources to support operations, planning, execution, and
 618 commander's decisions. The information, intelligence, products, and material obtained are
 619 refined for use in mission analysis, IPB, and planning through functional analysis. This subtask
 620 encompasses the military aspects of terrain.
- 621 • **Obtain Detailed Weather and Weather Effects Information and Intelligence.** Obtain
 622 detailed information and intelligence concerning the recent and historical weather trends,
 623 seasonal patterns, aspects of weather, and weather zones. Obtain information on how the
 624 weather affects friendly and enemy forces and operations in the AOI through intelligence reach;
 625 research; data mining; database access via the digital topographic support system; academic
 626 studies, products, or materials; intelligence archives; OSINT; or other information sources to
 627 support operations, planning, execution, and commander's decisions. The Integrated
 628 Meteorological System is accessed through DCGS-A and provides commanders at all echelons
 629 of command with an automated weather system. This system receives, processes, and
 630 disseminates weather observations, forecasts, and weather and environmental effects decision
 631 aids to all warfighting functions. The information, intelligence, products, and material obtained
 632 are refined for use in mission analysis, IPB, and planning through functional analysis. This
 633 subtask requires specific and detailed information for each weather factor.
- 634 • **Obtain Detailed Civil Considerations Information and Intelligence.** Obtain detailed
 635 information and intelligence concerning the civil considerations within or affecting the expected
 636 AOI through intelligence reach; research; data mining; database access; academic studies,
 637 products, or materials; intelligence archives; OSINT; or other information sources to support
 638 operations, planning, execution, and commander's decisions. The data, information, intelligence,
 639 products, and material obtained are refined for use in IPB, and planning through functional
 640 analysis. This subtask requires specific and detailed information for each factor.
- 641 • **Complete Studies.** Study and provide understanding of the local populations; cultures and caste
 642 system; societal systems or organizations; political systems and structures; religions practiced
 643 and their impacts; moral beliefs and their impacts; civil authority considerations; military
 644 organizations, structure, and equipment; and attitudes toward US, multinational, or HN forces to
 645 assist in achieving goals and objectives. Studies can also include the views and attitudes of
 646 multinational and HN forces towards these factors. The study provides detailed information,
 647 assessments, and conclusions on the AOIs of the requesting command or organization. The
 648 study could be a systems or functional analysis product and should be as detailed and in-depth
 649 as time allows. This subtask has two subtasks:
 - 650 ■ **Conduct Area, Regional, or Country Study of a Foreign Country.** Study and provide
 651 mission-focused understanding of the terrain, civil considerations, weather, and threat
 652 characteristics for a specified area or region of a foreign country, to include attitudes
 653 toward joint, multinational, or HN forces to assist in achieving goals and objectives. The
 654 studies can also include the views and attitudes of multinational and HN forces. The study

FOR OFFICIAL USE ONLY

655 provides detailed information, assessments, and conclusions on the AOIs of the requesting
656 command or organization and should be as detailed as time allows.
657 ■ **Conduct Specified Study.** Study and provide focused understanding of the terrain, civil
658 considerations, weather, and threat characteristics for a specified topic or requirement. The
659 study provides detailed information, assessments, and conclusions on the AOIs of the
660 requesting command or organization and should be as detailed and in-depth as time allows.

661 **Tailor the Intelligence Force**

662 1-47. The generating force uses mission analysis to focus the allocation of intelligence resources for use by
663 a joint task force (JTF) or combatant commander (CCDR) as well as to support strategic objectives, the
664 Army's mission, and operations at each echelon. Based on the mission analysis, the staff at each echelon
665 allocates intelligence resources obtained through the generating force to support the commander's
666 guidance, intent, and mission objectives.

667 **SUPPORT TO SITUATIONAL UNDERSTANDING**

668 1-48. Support to situational understanding is the task of providing information and intelligence to
669 commanders to assist them in achieving a clear understanding of the force's current state with relation to
670 the enemy and the environment. It supports the commander's ability to make sound decisions.

671 **Perform Intelligence Preparation of the Battlefield**

672 1-49. IPB is a continuous staff planning activity undertaken by the entire staff. The staff aims to
673 understand the operational environment and the options it presents to friendly and threat forces. IPB is a
674 systematic process of analyzing and visualizing the portions of the mission variables of threat, terrain,
675 weather, and civil considerations in a specific AOI and for a specific mission. By applying IPB,
676 commanders gain the information necessary to selectively apply and maximize combat power at critical
677 points in time and space.

678 **Perform Situation Development**

679 1-50. Situation development is a process for analyzing information and producing current intelligence
680 concerning the portions of the mission variables of enemy, terrain, weather, and civil considerations before
681 and during operations. The process helps the intelligence officer recognize and interpret indicators of threat
682 intentions, objectives, combat effectiveness, and potential COAs. Situation development confirms or denies
683 threat COAs, provides threat locations, explains what the threat is doing in relation to the friendly force
684 commander's intent, and provides an estimate of threat combat effectiveness. The locations and actions of
685 noncombatant elements and NGOs in the AO that may impact operations should also be considered.
686 Through situation development, the intelligence officer quickly identifies information gaps, explains threat
687 activities in relation to the unit's operations, and assists the commander in gaining and maintaining
688 situational understanding. Situation development helps the commander make decisions and execute
689 branches and sequels.

690 **Provide Intelligence Support to Protection**

691 1-51. Provide intelligence in support of protecting the Army's fighting potential so that it can be applied at
692 the appropriate time and place. This task includes those measures the command takes to remain viable and
693 functional by protecting itself from effects of or recovery from threat activities. This task is linked with
694 antiterrorism and homeland security.

695 **Provide Tactical Intelligence Overwatch**

696 1-52. Tactical intelligence overwatch is creating standing, fixed analytical intelligence capabilities that
697 provide dedicated intelligence support and overwatch to committed maneuver units. The tactical

FOR OFFICIAL USE ONLY

698 intelligence overwatch cell is connected via a shared intelligence network that can pull information from
 699 multiple sources and provide succinct answers directly to supported units when time is critical.

700 **Conduct Police Intelligence Operations**

701 1-53. Police intelligence is a set of systems, technologies, and processes that use data and information to
 702 analyze, understand, and focus policing operations and activities to achieve social order. Police intelligence
 703 operations (PIO) is a military police (MP) integrating function that supports the intelligence and protection
 704 warfighting functions through the integration of police engagement, police information, and police
 705 investigations to enhance situational understanding, protection of the force, and homeland security. This
 706 information, whether police, criminal, or tactical in nature, is gathered while conducting policing functions
 707 and upon analysis may contribute to CCIRs, intelligence-led, time-sensitive operations, or policing
 708 strategies necessary to forecast, anticipate, and preempt crime or related activities to maintain order.

709 1-54. The dissemination of police and criminal information is included in ART 5.5.1.2.3 (Conduct criminal
 710 investigations). Joint, interagency, and multination coordination is included in ART 5.2.2.1 (Prepare the
 711 Command Post for Displacement) (FM 3-19.1) (US Army Military Police School).

712 *Note.* The PIO function is not an intelligence discipline; it is a law enforcement function.
 713 However, it is within the critical intelligence task, “support situational understanding” that PIO
 714 best supports the MI cycle. Police intelligence operations are essential to this task, particularly
 715 where asymmetric threats (criminal, terrorist, and insurgents) threaten the security of US forces
 716 and military operations. This function supports and enhances the commander’s situational
 717 awareness and common operational picture (COP) through collection, analysis, and appropriate
 718 dissemination of relevant criminal, police information, and criminal intelligence. Police
 719 intelligence operations are a vital tool of law enforcement and criminal investigators that
 720 distributes and focuses MP and criminal investigations assets. US Codes, executive orders,
 721 Department of Defense (DOD) directives, and Army regulations contain specific guidance
 722 regarding the prohibition of intelligence personnel from collecting intelligence on US citizens,
 723 US corporations, and resident aliens. Any access by the intelligence community to information
 724 or products resulting from PIO directed against American citizens should undergo competent
 725 legal review.

726 **Provide Intelligence Support to Civil Affairs Operations**

727 1-55. This task enables MI organizations to collect and provide information and intelligence products
 728 concerning the factors of ASCOPE in the AO in support of civil affairs (CA) activities.

729 **PERFORM INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE**

730 1-56. ISR is an activity that synchronizes and integrates the planning and operation of sensors, assets, and
 731 processing, exploitation, and dissemination of systems in direct support (DS) of current and future
 732 operations. This is an integrated intelligence and operations function. For Army forces, this combined arms
 733 operation focuses on priority intelligence requirements (PIRs) while answering the CCIRs. Through ISR,
 734 commanders and staffs continuously plan, task, and employ collection assets and forces. These forces
 735 collect, process, and disseminate timely and accurate information, combat information, and intelligence to
 736 satisfy the CCIRs and other intelligence requirements. When necessary, ISR assets focus on special
 737 requirements, such as personnel recovery.

738 **Perform ISR Synchronization**

739 1-57. *Intelligence, surveillance, and reconnaissance synchronization is the task that accomplishes the*
 740 *following: analyzes information requirements and intelligence gaps; evaluates available assets*

FOR OFFICIAL USE ONLY

741 **internal and external to the organization; determines gaps in the use of those assets; recommends**
742 **intelligence, surveillance, and reconnaissance assets controlled by the organization to collect on the**
743 **commander's critical information requirements; and submits requests for information for adjacent**
744 **and higher collection support** (FM 3-0). This task ensures that ISR, intelligence reach, and requests for
745 information (RFIs) successfully report, produce, and disseminate information, combat information, and
746 intelligence to support decision making. The intelligence officer, in coordination with the operations
747 officer and other staff elements as required, synchronizes the entire collection effort. This effort includes
748 assets the commander controls and those of adjacent and higher echelon units and organizations. It also
749 uses intelligence reach to answer the CCIRs and other requirements. This task has two subtasks:

- 750 ● **Develop Information Requirements.** The intelligence staff develops a prioritized list focusing
751 on what information it needs to collect to produce intelligence. Additionally, the intelligence
752 staff dynamically updates and adjusts the requirements in response to mission adjustments and
753 changes. Each requirement is assigned a latest time information is of value (LTIOV) to meet
754 operational requirements.
- 755 ● **Develop the ISR Synchronization Plan.** The entire unit staff develops their information
756 requirements and determines how best to satisfy them. The staff uses reconnaissance and
757 surveillance assets to collect information. The intelligence synchronization plan includes all
758 assets that the operations officer can task or request and coordinating mechanisms to ensure
759 adequate coverage of the AOIs.

760 Perform ISR Integration

761 1-58. **Intelligence, surveillance, and reconnaissance integration is the task of assigning and controlling**
762 **a unit's intelligence, surveillance, and reconnaissance assets (in terms of space, time, and purpose) to**
763 **collect and report information as a concerted and integrated portion of operation plans and orders**
764 (FM 3-0). ISR integration assigns and controls a unit's ISR assets (in terms of space, time, and purpose) to
765 collect and report information as a concerted and integrated portion of operation plans (OPLANs) and
766 operations orders (OPORDs). The operations officer integrates the best ISR assets through a deliberate and
767 coordinated effort of the entire staff. Specific information requirements facilitate tasking by matching
768 requirements to assets. Intelligence requirements are identified, prioritized, and validated. ISR integration
769 is vital in controlling limited ISR assets. During ISR integration, the staff recommends redundancy, mix,
770 and cue as appropriate. The result of ISR synchronization and integration is an effort focused on answering
771 the commander's requirements. This task has two subtasks:

- 772 ● **Develop the ISR Plan.** The operations officer develops the ISR plan. The entire unit staff
773 analyzes each requirement to determine how best to satisfy it. The staff receives ISR tasks and
774 RFIs from subordinate and adjacent units and higher headquarters. The ISR plan includes all
775 assets that the operations officer can task or request and coordinating mechanisms to ensure
776 adequate coverage of the AOI.
- 777 ● **Execute, Evaluate, and Update the ISR Plan.** The operations officer updates the ISR plan
778 based on information received from the intelligence officer. The operations officer is the
779 integrator and manager of the ISR effort through an integrated staff process and procedures. As
780 PIRs are answered and new information requirements arise, the intelligence officer updates
781 intelligence synchronization requirements and provides the new input to the operations officer
782 who updates the ISR plan. The intelligence and operations officers work closely with all staff
783 elements to ensure the unit's collectors receive appropriate taskings. This ISR plan reflects an
784 integrated collection strategy and employment, production, and dissemination scheme that will
785 effectively answer the CCIRs. This task includes updating ISR operations through dynamic
786 retasking and periodic updates of the ISR plan.

787 Conduct Reconnaissance

788 1-59. Reconnaissance is a mission undertaken to obtain, by visual observation or other detection methods,
789 information about activities and resources of an enemy or potential enemy. This mission also secures data

FOR OFFICIAL USE ONLY

790 concerning the meteorological, hydrographic, or geographic characteristics and the local population of an
 791 AO. Other detection methods include signals, imagery, measurement of signature, or other technical
 792 characteristics. This task includes performing chemical, biological, radiological, and nuclear (CBRN)
 793 reconnaissance; engineer reconnaissance (to include infrastructure reconnaissance and environmental
 794 reconnaissance).

795 **Conduct Surveillance**

796 1-60. Surveillance is the systematic observation of aerospace, surface, or subsurface areas, places, persons,
 797 or things by visual, aural, electronic, photographic, or other means. Other means may include but are not
 798 limited to space-based systems, and using special CBRN, artillery, engineer, special operations forces, and
 799 air defense equipment. Surveillance involves observing an area to collect information.

800 **Conduct Related Missions and Operations**

801 1-61. The associated tasks (mission and debriefing program, intelligence coordination, technical channels,
 802 and intelligence support to personnel recovery) that facilitate the conduct of ISR operations and the
 803 specialized missions (sensitive site exploitation [SSE]), providing intelligence and information outside the
 804 traditional ISR construct. This task has four subtasks:

- 805 ● **Establish a Mission Intelligence Briefing and Debriefing Program.** The commander must
 806 establish, support, and allocate appropriate resources for a mission briefing and debriefing
 807 program. The battle updates and after-action reviews are separate tasks from the mission
 808 briefing and debriefing program. The G-2/S-2 develops a mission intelligence briefing plan and
 809 complementary debriefing plan to support the commander's program. The intelligence mission
 810 briefing plan sensitizes Soldiers to specific information and reporting requirements, information
 811 gaps, and unique mission requirements. The intelligence mission briefings and debriefings
 812 generally follow the format of a mission briefing: review the route traveled, collection objectives
 813 of the patrol, and methods employed. The debriefing program captures the SIRs the patrol was
 814 to collect and any additional information and observations the patrol made concerning the
 815 operational environment. It also collects any fliers, pamphlets, media, or pictures the patrol
 816 found or obtained. This subtask has two subtasks:
 - 817 ■ **Establish a Mission Intelligence Briefing Plan.** The G-2/S-2 section should develop a
 818 mission intelligence briefing plan. The mission intelligence briefing plan ensures that all
 819 Soldiers conducting patrols, tactical movements, and nontactical movements are sensitized
 820 to specific information and reporting requirements, information gaps, and unique mission
 821 requirements. The intelligence mission briefing and debriefing generally follow the format
 822 of a mission briefing: review the route traveled, collection objectives of the patrol, and
 823 methods employed.
 - 824 ■ **Establish a Debriefing Plan.** The G-2/S-2 section develops a complementary debriefing
 825 plan. The debriefing plan captures the SIRs the patrol was to collect and any additional
 826 information and observations the patrol made concerning the operational environment. It
 827 also collects any fliers, pamphlets, media, or pictures the patrol found or obtained. The
 828 program should include all returning patrols, leaders who have traveled to meetings,
 829 returning human intelligence (HUMINT) collection teams (HCTs), aircrews, and others
 830 who may have obtained information of intelligence value. The G-2/S-2 section debriefs
 831 personnel, writes and submits reports, or reports information verbally, as appropriate. The
 832 requirement for a debriefing by the G-2/S-2 section following each mission should be a part
 833 of the intelligence mission briefing. Leaders should not consider the mission complete and
 834 release the personnel until the reporting and debriefings are done.
- 835 ● **Conduct Intelligence Coordination.** Conduct intelligence coordination is the task carried out
 836 by the intelligence section to facilitate active collaboration horizontally, laterally, and vertically.
 837 It includes providing and conducting technical channels to refine and focus the intelligence

FOR OFFICIAL USE ONLY

838 disciplines ISR tasks. It also properly coordinates the discipline assets when operating in another
839 unit's AO. This subtask has two subtasks:

- 840 ■ **Establish and Maintain Technical Channels.** Intelligence commanders and the
841 intelligence staff maintain control of each intelligence discipline during operations through
842 technical channels to ensure adherence to applicable laws and policies, ensure proper use of
843 doctrinal techniques, and provide technical support and guidance. Applicable laws and
844 policies include all relevant US law, the law of war, international law, directives, DOD
845 Instructions, and Orders. Commanders direct operations but often rely on technical
846 expertise to plan, prepare, execute, and assess portions of the unit's collection effort.
847 Technical channels also involve translating ISR tasks into the specific parameters used to
848 focus highly technical or legally sensitive aspects of the ISR effort. Technical channels
849 include but are not limited to defining, managing, or guiding the use of specific ISR assets;
850 identifying critical technical collection criteria such as technical indicators; recommending
851 collection techniques, procedures, or assets; coordinating operations; and directing
852 specialized training for specific MI personnel or units.

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

- 855 ■ **Conduct Deconfliction and Coordination.** Deconfliction and coordination consists of a
856 series of related activities that facilitate operations in another unit's AO. These activities
857 facilitate successful ISR collection, support of the mission, and fratricide avoidance.
858 Military intelligence organizations may be used in general support for coverage of an AO
859 or in DS to support a specific unit. Military intelligence organizations operating in general
860 support should coordinate with unit commanders when operating in that unit's AO. At a
861 minimum, the MI organizations announce their presence and request information on any
862 conditions or ongoing situations that may affect how they conduct their mission. An MI
863 organization operating in DS of a specific unit coordinates with the unit for augmentation
864 to conduct operations in accordance with FP requirements. The MI organization's leader
865 also coordinates with the supported unit's S-2 for debriefings of returning members,
866 convoy leaders, and others.

867 **Support Sensitive Site Exploitation**

868 1-62. SSE consists of a related series of activities inside a captured sensitive site to exploit personnel,
869 documents, electronic data, and material captured at the site, while neutralizing any threat posed by the site
870 or its contents. A sensitive site is a designated, geographically limited area with special diplomatic,
871 informational, military, and economic sensitivity for the United States. This includes factories with
872 technical data on enemy weapon systems, war crimes sites, critical hostile government facilities, areas
873 suspected of containing persons of high rank in a hostile government or organization, terrorist money
874 laundering areas, and document storage areas for secret police forces. These activities exploit personnel,
875 documents, electronic data, and material captured at the site while neutralizing any threat posed by the site
876 or its contents. While the physical process of exploiting the sensitive site begins at the site itself, full
877 exploitation may involve teams of experts located around the world.

878 **Intelligence Support to Personnel Recovery**

879 1-63. Support to personnel recovery consists of intelligence activities and capabilities focused on
880 collecting information to recover and return own personnel—whether Soldier, Army civilian, selected
881 DOD contractors, or other personnel as determined by the Secretary of Defense—who are isolated,
882 missing, detained, or captured in an operational environment. This support also includes detailed analysis,
883 developing detailed products, and estimates to support operations undertaken to recover isolated, missing,
884 detained, or captured personnel.

FOR OFFICIAL USE ONLY

885 **SUPPORT TO TARGETING AND INFORMATION SUPERIORITY**

886 1-64. Intelligence support to targeting and information superiority is the task of providing the commander
887 information and intelligence support for targeting through lethal and nonlethal actions. It includes
888 intelligence support to the planning and execution of direct and indirect fires, command and control
889 engagement, information engagement, and individual capabilities of information operations as well as
890 assessing the effects of those operations.

891 **Provide Intelligence Support to Targeting**

892 1-65. The intelligence officer (supported by the entire staff) provides the fire support coordinator,
893 information engagement officer, electronic warfare (EW) officer, and the information operations officer
894 with information and intelligence for targeting the threat's forces and systems with direct and indirect
895 lethal and nonlethal fires. It includes identification of threat capabilities and limitations. The targeting
896 process uses the decide, detect, deliver, and assess (D3A) methodology. The intelligence officer ensures
897 the ISR plan supports the finalized targeting plan. This task has two subtasks:

- 898 ● **Provide Intelligence Support to Target Development.** The systematic analysis of threat forces
899 and operations to determine high-value targets (HVTs) (people, organizations or military units),
900 high-payoff targets (HPTs) (people, organizations or military units), and systems and system
901 components for potential attack through maneuver, fires, electronic means, or information
902 engagement or operations.
- 903 ● **Provide Intelligence Support to Target Detection.** The intelligence officer establishes
904 procedures for dissemination of targeting information. The targeting team develops the sensor
905 and attack guidance matrix to determine the sensor required to detect and locate targets. The
906 intelligence officer places these requirements into the ISR synchronization plan for later
907 incorporation into the ISR plan.

908 **Provide Intelligence Support to Information Superiority**

909 1-66. Intelligence support to targeting and information superiority is the task of providing the commander
910 information and intelligence support for targeting through lethal and nonlethal actions. It includes
911 intelligence support to the planning and execution of direct and indirect fires, command and control
912 engagement, information engagement, and individual capabilities of information operations as well as
913 assessing the effects of those operations. Key activities reflected in this task include communications,
914 planning, synchronization, and integration of intelligence into OPLANs and OPORDs. This task has five
915 subtasks:

- 916 ● **Provide Intelligence Support to Information Engagement.** The intelligence warfighting
917 function when operating outside US territories supports activities related to information
918 engagement under some circumstances. This subtask has two subtasks:
 - 919 ■ **Provide Intelligence Support to Public Affair.** This task enables MI organizations to
920 collect and provide information and intelligence products concerning civil considerations in
921 the operational environment in support of public affairs (PA) activities.
 - 922 ■ **Provide Intelligence Support to Psychological Operations.** Psychological operations
923 (PSYOP) require information and intelligence to support analysis of foreign target
924 audiences and their environment to include the PMESII-PT factors. Continuous and timely
925 intelligence are required to assess target audience behavioral trends. Information and
926 intelligence are centered on target audience motivation and behavior; the analysis of
927 collected impact indicators; and the target audience's reaction to friendly, hostile, and
928 neutral force actions.
- 929 ● **Provide Intelligence Support to Command and Control Warfare.** The intelligence
930 warfighting function supports command and control warfare by providing information to
931 identify threat decision making and command and control nodes, processes, and means by order
932 of criticality. Intelligence also helps identify threat systems, activities, and procedures that may

FOR OFFICIAL USE ONLY

933 be vulnerable to command and control warfare. Additionally, intelligence plays a key role in
934 evaluating and assessing the effectiveness of command and control warfare.

935 *Note.* This task supports electronic attack (EA) employing jamming, electromagnetic energy, or
936 directed energy against personnel, facilities, or equipment. It identifies critical threat information
937 systems and command and control nodes.

- 938 ● **Provide Intelligence Support to Information Protection.** The intelligence warfighting
939 function supports information protection by providing information to identify threat offensive
940 information operations capabilities and activities and tactics, techniques, and procedures (TTP).
941 Intelligence provides information relating to computer network defense, physical security,
942 OPSEC, counterdeception, and counterpropaganda.
- 943 ● **Provide Intelligence Support to Operations Security.** This task identifies capabilities and
944 limitations of the threat's intelligence system including adversary intelligence objectives and
945 means, procedures, and facilities to collect, process, and analyze information. This task supports
946 the identification of indicators that adversary intelligence capabilities and systems might obtain
947 that could be interpreted or pieced together to obtain essential elements of friendly information
948 in time to be useful to adversaries.
- 949 ● **Provide Intelligence Support to Military Deception.** This task identifies capabilities and
950 limitations of the threat's intelligence-collecting capabilities, systems, and means and identifies
951 threat biases and perceptions.

952 **Provide Intelligence Support to Combat Assessment**

953 1-67. Intelligence supports the assess phase of the operations process and targeting methodology. The
954 commander uses combat assessment to determine if targeting actions have met the attack guidance and if
955 reattack is necessary to perform essential fires tasks and achieve the commander's intent for fires. The staff
956 determines how combat assessment relates to specific targets by completing battle damage, physical
957 damage, functional damage, and target system assessments. This task has two subtasks:

- 958 ● **Conduct Physical Damage Assessment.** This is a staff task that estimates the extent of physical
959 damage to a target based on observed or interpreted damage. It is a post-attack target analysis
960 that is a coordinated effort among all units.
- 961 ● **Conduct Functional Damage Assessment.** The staff conducts the functional damage
962 assessment for the remaining functional or operational capability of the threat. The assessment
963 focuses on measurable effects and estimates the threat's ability to reorganize or find alternative
964 means to continue operations. The targeting cell and staff integrate analysis with external
965 sources to determine if the commander's intent for fires has been met.

966 **CHARACTERISTICS OF EFFECTIVE INTELLIGENCE**

967 1-68. The effectiveness of the intelligence warfighting function is measured against the relevant
968 information quality criteria:

- 969 ● **Accuracy.** Intelligence must give commanders an accurate, balanced, complete, and objective
970 picture of the enemy and the operational environment. To the extent possible, intelligence
971 should accurately identify threat intentions, capabilities, limitations, and dispositions. It should
972 be derived from multiple sources and disciplines to minimize the possibility of deception or
973 misinterpretation. Alternative or contradictory assessments should be presented, when
974 necessary, to ensure balance and bias-free intelligence.
- 975 ● **Timeliness.** Intelligence must be provided early enough to support operations, and prevent
976 surprise from enemy action. It must flow continuously to the commander before, during, and
977 after an operation. Intelligence organizations, databases, and products must be available to
978 develop estimates, make decisions, and plan operations.

FOR OFFICIAL USE ONLY

- 979 ● **Usability.** Intelligence must be presented in a form that is easily understood or displayed in a
980 format that immediately conveys the meaning to the consumer.
- 981 ● **Completeness.** Intelligence briefings and products must convey all the necessary components to
982 be as complete as possible.
- 983 ● **Precision.** Intelligence briefings and products must provide the required level of detail to
984 answer the requirements, no more and no less.
- 985 ● **Reliability.** Intelligence must be evaluated to determine the extent to which the information that
986 has been collected and is being used in intelligence briefings and products is trustworthy,
987 uncorrupted, and undistorted. If there are any concerns with these, they must be stated up front.
- 988 1-69. Intelligence requires three additional criteria in order to be effective:
- 989 ● **Relevant.** Intelligence must support the commander's concept of the operation and the unit's
990 mission. It must be relevant to the capabilities of the unit, the CCIRs, and the commander's
991 preferences.
- 992 ● **Predictive.** Intelligence should inform the commander about what the enemy can do (most
993 dangerous COA), and is most likely expected to do (most likely enemy COA). The intelligence
994 warfighting function should anticipate the intelligence needs of the commander.
- 995 ● **Tailored.** Intelligence must be presented based on the needs of the commanders, subordinate
996 commanders, and staff in a specific format that is clear and concise so they can understand it,
997 believe it, and act on it. It should support and satisfy the priorities of the commander.

998 **ACTIONABLE INTELLIGENCE**

- 999 1-70. Actionable intelligence is an example of bringing the characteristics of effective intelligence together
1000 with the effective integration of intelligence into ongoing operations to support the commander. Joint
1001 doctrine discusses the concept of critical intelligence. (See JP 2-0.) Army personnel have used the concept
1002 of actionable intelligence to reflect the Joint concept of critical intelligence. In the current operational
1003 environment, the concept of actionable intelligence is used by Army personnel to describe information that
1004 answers operational requirements or specific commander's guidance in the attack guidance matrix to
1005 sufficient degree and with sufficient reliability to support the commander's targeting decisions.
- 1006 1-71. Ideally, the staff thoroughly integrates intelligence into the operations process for all operations to
1007 ensure the collection and reporting of timely, relevant, accurate, predictive, and tailored information and
1008 intelligence. This is accomplished by using the characteristics of effective intelligence as well as
1009 conducting successful ISR operations through detailed ISR synchronization and integration so that
1010 commanders can fight the threat through knowledge rather than assumption.

1011 **THE INTELLIGENCE PROCESS**

- 1012 1-72. Intelligence operations are executed by performing five steps that constitute the intelligence process:
1013 generate intelligence knowledge, plan, prepare, collect, and produce. Additionally, there are three activities
1014 that occur across the five steps of the intelligence process: analyze, assess, and propagate. The three
1015 continuing activities plus the commander's input drive, shape, and develop the process; they can occur at
1016 any time during the process.
- 1017 1-73. The intelligence process provides a common model with which to guide one's thoughts, discussions,
1018 plans, and assessments. The intelligence process generates information, products, and knowledge about the
1019 threat, terrain and weather, and civil considerations, which supports the commander and staff in the
1020 conduct of operations. Figure 1-1 shows the intelligence process.

FOR OFFICIAL USE ONLY

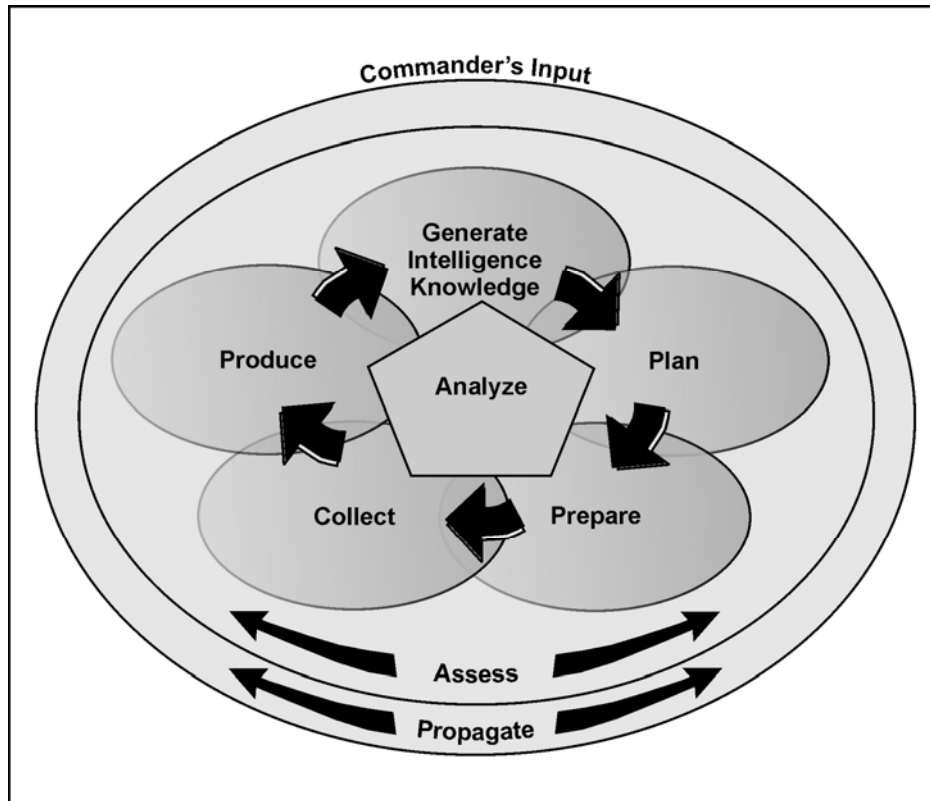


Figure 1-1. The intelligence process

1021

1022 **GENERATE INTELLIGENCE KNOWLEDGE**

1023 1-74. Generate intelligence knowledge is a continuous and user-defined step driven by the commander that
 1024 begins prior to mission receipt and provides the relevant knowledge required concerning the operational
 1025 environment for the conduct operations. Generate intelligence knowledge begins as early as possible, in
 1026 some cases when the commander knows only the general location or category of mission for a projected
 1027 operation, and continues throughout the operations process. The unit determines what information it will
 1028 need (based on the commander's guidance), what information it already has, and what information it needs
 1029 to collect. For Army units, the initial step in locating the information they need to collect will be
 1030 establishing an intelligence architecture that provides access to relevant intelligence community and other
 1031 DOD databases and data files. When conducting the generate intelligence knowledge step, units and
 1032 personnel must follow all applicable policies and regulations on the collection of information and OPSEC.
 1033 Generate intelligence knowledge is an integral part of the intelligence process. (When published, refer to
 1034 TC 2-33.401.)

1035 **Initial Database Development**

1036 1-75. The initial result of the generate intelligence knowledge step is the creation and population of data
 1037 files as directed by the commander that are compatible with the unit's battle command systems. When
 1038 generating intelligence knowledge, unit intelligence personnel should begin by determining what
 1039 information they need to collect based on the primary components of the operational environment for
 1040 which the intelligence staff is responsible in order to support the command, IPB, and answer the CCIRs.

FOR OFFICIAL USE ONLY

1041 1-76. As units begin to collect data on the projected AO, the data should be organized into baseline data
 1042 files per the commander's guidance. Generally, the tactical echelons create primary data files, based on the
 1043 threat, terrain, weather, and civil considerations. Strategic and operational echelons create data files based
 1044 on the commander's operational requirements. Information can be based on the joint system's perspective
 1045 (PMESII), as well as the operational variables (PMESII-PT) to populate the baseline data files.

1046 1-77. All-source analysts ensure that relevant information is incorporated into the common database and
 1047 the unit webpage. This information becomes the basis for providing intelligence support for developing
 1048 predeployment readiness training on the operational environment. This information is used to develop
 1049 Soldier predeployment packages; it helps to identify the specific types of threats, threat equipment, and
 1050 threat TTP and civil considerations that Soldiers can expect to encounter when deployed. This information
 1051 can be used to incorporate simulations or replications of items such as threat vehicles, weapons, and
 1052 uniforms as well as threat TTP—along with civil considerations in the AO—into predeployment training
 1053 exercises or mission rehearsal exercises to provide the most realistic and relevant training possible.

1054 1-78. As with IPB, generate intelligence knowledge is a continuous process. Many factors can drive the
 1055 requirement to update the baseline knowledge. This can include current operations, higher operations,
 1056 intelligence analysis or assessments, and additional considerations. Additional considerations include such
 1057 factors as updates based on local elections or key local leadership personnel changes, changes to local
 1058 infrastructure, and events outside the unit's projected AO that may impact operations within the projected
 1059 AO.

1060 1-79. After creating the data files the data, information, intelligence, products, and material obtained are
 1061 organized and refined to support planning. Generate intelligence knowledge is the precursor for conducting
 1062 IPB and mission analysis. Generate intelligence knowledge is also the basis for developing a unit's initial
 1063 intelligence survey. (When published, see TC 2-33.401 and FM 3-0.2) The generate intelligence
 1064 knowledge process continues to gather, categorize, and analyze information on relevant aspects of the
 1065 projected AO, continually adding new information and updating and refining the understanding of the
 1066 projected AO throughout the operations process.

1067 1-80. During a deployment, a unit's information databases become a source of information for the generate
 1068 intelligence knowledge step of follow-on units (in support of Army Force Generation [ARFORGEN]) that
 1069 may replace them. During and after deployment, the generate intelligence knowledge step also supports
 1070 tactical overwatch and the collection of lessons learned.

1071 **Intelligence Survey**

1072 1-81. The intelligence survey is a process that assists the G-2/S-2 in identifying ISR asset collection
 1073 capabilities and limitations within the projected AO for potential employment. The intelligence survey
 1074 consists of five steps:

- 1075 ● Develop a comprehensive information baseline, collection capability baseline, and analytical
 1076 baseline for the projected AO.
- 1077 ● Determine key intelligence gaps.
- 1078 ● Determine key gaps in analytical ability.
- 1079 ● Develop an understanding of the information and intelligence that can be collected with unit
 1080 intelligence assets and, when appropriate, ISR assets in the projected AO and how and where it
 1081 may best be collected.
- 1082 ● Determine a method of understanding when changes to the information baseline, collection
 1083 capability baseline, or analytical baseline occur that are of intelligence interest.

1084 1-82. The intelligence survey, which is developed over time and is continuously updated, provides the unit
 1085 intelligence officer with an initial assessment for recommending intelligence asset apportionment within
 1086 the projected AO and how best to use the unit's intelligence assets within the projected AO, taking into
 1087 account technical and tactical considerations across all disciplines. For example, one portion of the
 1088 projected AO may be unsuited for unit SIGINT asset collection due to terrain or lack of threat transmitters,

FOR OFFICIAL USE ONLY

1089 but it may be well-suited for HUMINT collection teams (HCTs). The intelligence officer may recommend
1090 to the commander that unit SIGINT collection assets not be deployed to that area, but that additional HCTs
1091 would be a valuable source of intelligence collection in that same area.

1092 1-83. This assessment includes determining what nonstandard ISR assets, to include quick reaction
1093 capabilities and off-the-shelf capabilities and systems, are available to support the commander.
1094 Additionally, when reviewing contingency plans (CONPLANS) and operations plans (OPLANS), the
1095 G-2/S-2 should use the intelligence survey to update the CONPLAN or OPLAN based on new
1096 technologies, capabilities, or sources of information and intelligence.

1097 1-84. The intelligence survey also assists in determining what communications will be required for
1098 deployed intelligence operations and addresses any apparent gaps in intelligence standing operating
1099 procedures (SOPs). Additionally, the intelligence survey is the basis for determining what additional or
1100 specialized intelligence assets the unit may require for mission accomplishment.

1101 **PLAN**

1102 1-85. The plan task consists of the activities that identify pertinent information requirements and develop
1103 the means for satisfying those requirements. The CCIRs (PIRs and FFIRs) drive the ISR effort. The
1104 intelligence officer synchronizes ISR operations and supports the G-3/S-3 in ISR integration. Planning
1105 activities include, but are not limited to—

- 1106 ● Conducting IPB and preparing IPB products and overlays.
- 1107 ● Developing initial PIRs.
- 1108 ● Developing the ISR synchronization plan, overlays, and matrices.
- 1109 ● Developing the initial running intelligence estimates or briefings (usually as part of the Mission
1110 Analysis Briefing), which should include initial PIRs as well as threat strengths and
1111 vulnerabilities that friendly forces should avoid or exploit.
- 1112 ● Managing requirements.
- 1113 ● Submitting RFIs and using intelligence reach to fill information gaps.
- 1114 ● Evaluating reported information.
- 1115 ● Establishing the intelligence communications and dissemination architecture.
- 1116 ● Developing, managing, and revising the ISR synchronization plan and the ISR plan as mission
1117 requirements change.
- 1118 ● Supporting the preparation of annex B (Intelligence), and assisting the S-3 in completing annex
1119 L (ISR).

1120 **PREPARE**

1121 1-86. Preparation is the key to successful intelligence analysis and collection. Intelligence analysts must
1122 use the previous steps to prepare products for the commander and staff for orders production and the
1123 conduct of operations. Failure to properly prepare for intelligence collection and the publication of finished
1124 intelligence products can cause an operation to be focused on an entirely wrong location, force, or
1125 objective. Thorough preparation by the staff allows the commander to focus the unit's power to achieve
1126 mission success. The prepare step includes those staff and leader activities which take place upon receiving
1127 the operations order (OPORD), OPLAN, warning order (WARNO), or commander's intent in order to
1128 improve the unit's ability to execute tasks or missions.

1129 **COLLECT**

1130 1-87. The collect task involves collecting, processing, and reporting information in response to ISR tasks.
1131 ISR assets collect information and data about the threat, terrain and weather, and civil considerations for a
1132 particular AO and AOI. A successful ISR effort results in the timely collection and reporting of relevant
1133 and accurate information which supports the commander's situational understanding.

FOR OFFICIAL USE ONLY

1134 1-88. This collected information forms the foundation of intelligence databases, intelligence production,
1135 and the situational awareness of the G-2/S-2. The requirements manager evaluates the reported information
1136 for its responsiveness to the CCIRs (PIRs and FFIRs).

1137 **Process**

1138 1-89. Once information has been collected, it is processed. Processing involves converting, evaluating,
1139 analyzing, interpreting, and synthesizing raw collected data and information into a format which enables
1140 the analysts to extract essential information to produce intelligence and targeting data. Examples of
1141 processing include preparing imagery for exploitation, enhancing imagery, translating a document from a
1142 foreign language, converting electronic data into a standardized reporting format (to include a database
1143 format) that can be analyzed by a system operator, and correlating information.

1144 1-90. Processing data and information is performed unilaterally and cooperatively by both humans
1145 (cognitive) and automated systems. Information or intelligence that is relevant to the current situation is
1146 converted into the appropriate format for inclusion in the common operational picture (COP).

1147 **Reporting**

1148 1-91. The timely and accurate reporting of combat information and intelligence is critical to successful
1149 operations. Information and intelligence is delivered as voice, text, graphic, or digital media. Voice data is
1150 reported over tactical radios on the command net or operations and intelligence net. Text, graphic, and
1151 other digital media are reported over the battle command network by system to include DCGS-A and
1152 deposited in the common database, email accounts, and on the unit's webpage.

1153 **PRODUCE**

1154 1-92. The produce task involves combining analyzed information and intelligence from single or multiple
1155 sources into intelligence or intelligence products in support of known or anticipated requirements.
1156 Production also involves combining new information and intelligence with existing intelligence in order to
1157 produce intelligence in a form that the commander and staff can apply to the military decision-making
1158 process (MDMP) and that supports and helps facilitate situational understanding. During the produce task,
1159 the intelligence staff exploits information by—

- 1160 ● Analyzing the information to isolate significant elements.
- 1161 ● Evaluating the information to determine accuracy, timeliness, usability, completeness, precision,
1162 and reliability. It must also be evaluated to determine if it is relevant, predictive, and properly
1163 tailored.
- 1164 ● Combining the information with other relevant information and previously developed
1165 intelligence.
- 1166 ● Applying the information to estimate possible outcomes.
- 1167 ● Presenting the information in a format that will be most useful to its user.

1168 1-93. The intelligence staff deals with numerous and varied production requirements based on PIRs and
1169 intelligence requirements; diverse missions, environments, and situations; and user format requirements.
1170 Through analysis, collaboration, and intelligence reach, the G-2/S-2 and the staff use the collective
1171 intelligence production capability of higher, lateral, and subordinate echelons to meet the production
1172 requirements. Proficiency in these techniques and procedures facilitates the intelligence staff's ability to
1173 answer command and staff requirements regardless of the factors of METT-TC.

1174 **CONTINUING ACTIVITIES**

1175 1-94. The three continuing activities discussed below drive, shape, and develop the process; they can occur
1176 at any time during the process.

FOR OFFICIAL USE ONLY

1177 **ANALYZE**

1178 1-95. *Analysis is the process by which collected information is evaluated and integrated with existing*
1179 *information to produce intelligence that describes the current—and attempts to predict the future—impact*
1180 *of the threat, terrain and weather, and civil considerations on operations (FM 2-33.4). The intelligence*
1181 *staff analyzes intelligence and information about the threat’s capabilities, friendly vulnerabilities, and the*
1182 *AO to determine how they will impact operations. The intelligence staff must also analyze and identify*
1183 *issues and problems that occur while conducting the unit’s intelligence process. One example of this could*
1184 *be focusing on the wrong priority or assets that are inadequately placed to collect required information.*

1185 1-96. This analysis enables the commander and staff to determine the appropriate action or reaction and to
1186 focus or redirect assets and resources to fill information gaps, mitigate collection limitations, or alleviate
1187 pitfalls.

1188 **Critical Thinking**

1189 1-97. Critical thinking is an essential element of the analytical thought process and is necessary for
1190 adaptation to new developments in the ever-changing combat environment. Rapid and constant changes in
1191 society and the uncertainties of future operations cause the military to realize the importance of critical
1192 thinking skills training

1193 1-98. *Critical thinking is the intellectually disciplined process of actively and skillfully conceptualizing,*
1194 *applying, analyzing, synthesizing, and/or evaluating information obtained from, or generated by,*
1195 *observation, experience, reflection, reasoning, or communication, as a guide to belief and action*
1196 *(FM 2-33.4). In its exemplary form, it is based on universal intellectual values that transcend subject matter*
1197 *divisions: clarity, accuracy, precision, consistency, relevance, sound evidence, good reasons, depth,*
1198 *breadth, and fairness.*

1199 1-99. Critical thinking involves improving the quality of thinking by applying the scientific elements of
1200 reasoning to gather, evaluate, and use information effectively. It consists of mental processes of
1201 discernment, analysis, and evaluation. It includes possible processes of reflecting upon a tangible or
1202 intangible item in order to form a solid judgment that reconciles scientific evidence with common sense.
1203 Hence, critical thinking is self-directed, self-disciplined, self-monitored, and self-corrective thinking. It
1204 requires effective communication, problem-solving abilities, and continuous evaluation.

1205 1-100. Critical thinking entails the examination of those structures or elements of thought implicit in all
1206 reasoning: purpose problem or question-at-issue, assumptions, concepts, empirical grounding, reasoning
1207 leading to conclusions, implications and consequences, objections from alternative viewpoints, and frame
1208 of reference. Critical thinking—in being responsible to variable subject matter, issues, and purposes—is
1209 incorporated in a family of interwoven modes of thinking, among them: scientific thinking, mathematical
1210 thinking, historical thinking, anthropological thinking, economic thinking, moral thinking, and
1211 philosophical thinking.

1212 1-101. The following are characteristics of a Critical Thinker:

- 1213 ● **Fair-minded.** Neutral in appraising or applying counter-theories to opinions of others.
- 1214 ● **Honest.** Must know and acknowledge personal biases and opinions.
- 1215 ● **Reasonable.** Applies checks and balances to a hypothesis to ensure it is possible.
- 1216 ● **Systematic.** Applies a methodical process to present ideas or concepts in a logical manner.
- 1217 ● **Precise.** Possesses the highest standard of accuracy.
- 1218 ● **Persistent.** Stays the course; does not stop at the obvious; digs deeper to overcome initial
- 1219 *conclusions, satisfied only when the hypothesis is fully developed.*
- 1220 ● **Focused.** Not easily swayed or distracted by emotions; maintains a point of concentration.
- 1221 ● **Questioning.** Not satisfied with the obvious; eager to seek out additional information and data
- 1222 *when none is immediately apparent.*

FOR OFFICIAL USE ONLY

- 1223 ● **Open-minded.** Willing to consider new or different ideas and modify the conclusions based
1224 upon new data or ideas even when they disagree with others.

1225 **CIVIL CONSIDERATIONS AND CULTURAL AWARENESS**

1226 1-102. Civil considerations comprise six characteristics expressed in the memory aid ASCOPE.
1227 Depending on the echelon conducting operations, these factors may be expressed using the joint systems
1228 perspective, the operational variables, and the mission variables. Additionally, the human terrain analysis
1229 team can provide detailed information and analysis pertaining to the socio-cultural factors involved in the
1230 operation.

1231 *Note.* For additional information on ASCOPE and the IPB process, see FM 2-01.3. Also refer to
1232 the operational variables (PMESII-PT) discussed in paragraph 1-2.

1233 1-103. A key component that describes the people is cultural awareness. Culture is the shared beliefs,
1234 values, customs, behaviors, and artifacts members of a society use to cope with the world and each other.
1235 Individuals belong to multiple groups through birth, assimilation, or achievement. Each group to which
1236 individuals belong influences their beliefs, values, attitudes, and perceptions. As such, culture is
1237 internalized in the sense that it is habitual, taken for granted, and perceived as natural by people in the
1238 society.

1239 1-104. Culture conditions an individual's range of action and ideas, including what to do and not do, how
1240 to do or not do it, and with whom to do it or not do it. Culture also includes the circumstances under which
1241 rules shift and change. Culture influences how people make judgments about what is right and wrong,
1242 assess what is important and unimportant, categorize things, and deal with things that do not fit into
1243 existing categories. Culture provides the framework for rational thought and decisions. What one culture
1244 considers rational may not be rational in another culture.

1245 1-105. Understanding other cultures applies to full spectrum operations, not just those dominated by
1246 stability. For example, different tactics may be used against an adversary who considers surrender a
1247 dishonor worse than death, as compared to those for whom surrender remains an honorable option.
1248 Cultural understanding is crucial to the success of multinational operations. Army leaders take the time to
1249 learn customs and traditions as well as the operational procedures and doctrine of their multinational
1250 partners and that of the HN. To operate successfully in multinational settings, Army leaders must recognize
1251 any differences in doctrinal terminology as well as the interpretation of orders and instructions. They must
1252 learn how and why others think and act as they do.

1253 **ASSESS**

1254 1-106. Assess plays a critical role in evaluating the information collected during the intelligence process.
1255 The continual assessment of ISR operations, available information and intelligence, and various aspects of
1256 the factors of METT-TC are critical to ensure that the intelligence staff:

- 1257 ● Answers the CCIRs.
1258 ● Provides the operations staff with input to redirect ISR assets in support of changing
1259 requirements.
1260 ● The effective use of information and intelligence.

1261 **PROPAGATE**

1262 1-107. Propagate includes direct dissemination; granting access to databases, information, or intelligence;
1263 and sharing. It also encompasses posting information to the web, intelligence reach, and updating the COP.

FOR OFFICIAL USE ONLY

1264 **Dissemination**

1265 1-108. Dissemination is the act of getting relevant information to the right person at the right time.
1266 Dissemination entails delivering timely, relevant, accurate, predictive, and tailored intelligence to the
1267 commander. Determining the product format and selecting the means to deliver it are key aspects of
1268 dissemination.

1269 1-109. Information presentation may be in a verbal, written, interactive, or graphic format. The type of
1270 information, the time allocated, and the individual preference of the commander all influence the
1271 information format. The DCGS-A enterprise provides a common backbone for the dissemination of
1272 intelligence. Answers to CCIRs for the commander, subordinate commanders, and staff require direct
1273 dissemination.

1274 **Granting Access**

1275 1-110. Granting access to databases, information, or intelligence ensures that personnel, units, or
1276 organizations that need all or part of the information in established classified and unclassified databases,
1277 programs, networks, systems, and other web-based collaborative environments for National Agency,
1278 Multinational, Joint, and Army organizations or echelons receive the appropriate access. This is
1279 accomplished through applicable National Agencies, Multinational, Joint, and Army regulations, policies,
1280 and procedures for personnel accesses and clearances; individual system accreditation; specialized training
1281 for clearances and systems or database usage; and special security procedures and enforcement.

1282 **Sharing**

1283 1-111. Sharing is primarily the result of establishing a web-based collaborative environment.
1284 Collaboration is the sharing of knowledge, expertise, and information normally online. Collaboration may
1285 take numerous forms. Collaborative tools are computer-based tools (groupware) that help individuals work
1286 together and share information. They allow for virtual online meetings and data sharing. Sharing allows
1287 analysts, other intelligence personnel, and other subject matter experts to freely exchange information and
1288 intelligence in support of answering their commander's requirements.

1289 **Posting**

1290 1-112. Information may be posted to the web for the widest possible dissemination. This makes the
1291 information available to personnel and units interested in the information or intelligence which is not part
1292 of the normal dissemination group for a specific unit or organization. When posting information to the web
1293 or updating information on their website, it is critical that units or organizations inform higher, subordinate,
1294 and lateral units or organizations that may require this information since units rarely have enough
1295 personnel to dedicate a Soldier to continuously search websites for new or updated information that may be
1296 of use to that unit or organization.

1297 **Intelligence Reach**

1298 1-113. Intelligence reach is an important part of the intelligence effort. Intelligence reach allows
1299 intelligence analysts to retrieve existing information, intelligence products, and data which can support
1300 answering the CCIRs from outside the unit in a timely manner without having to wait for an answer to an
1301 RFI or an ISR task. The information, intelligence products, or data retrieved can then be evaluated for use
1302 in the unit's intelligence products or analysis.

1303 **Updating the COP**

1304 1-114. As required by unit SOPs, new or updated intelligence information must be regularly inputted in
1305 the COP to provide the most current picture. The COP is a single display of all relevant information
1306 conveyed through reports, automatic updates, and overlays common to all echelons and digitally stored in a

FOR OFFICIAL USE ONLY

1307 common database. It facilitates battle command through collaborative interaction and real-time sharing of
1308 information between commanders and staffs. The intelligence portions of the COP are those messages and
1309 overlays relating to threat, terrain and weather, and civil considerations sent to the common database from
1310 intelligence organizations at various echelons and combat information transmitted from individual Soldiers
1311 and platforms. The G-2/S-2 monitors the common database to ensure it reflects the most current
1312 information and intelligence available.

1313 **COMMANDER'S INPUT**

1314 1-115. While commander's input is a commander's responsibility to drive the intelligence process, it is
1315 not a part of the intelligence process itself. Commander's input provides the primary mechanism for the
1316 commander to focus the intelligence warfighting function and is provided at the commander's discretion.
1317 Through the assess continuing activity, the intelligence staff is triggered to consult the commander to gain
1318 the commander's input. The commander's input directly influences the unit's ISR effort. Each commander
1319 determines which intelligence products are developed as well as the format of the products. The
1320 commander may provide input at any point during the intelligence process, and the intelligence effort will
1321 have to be adjusted accordingly.

1322 **ARMY INTELLIGENCE ENTERPRISE**

1323 1-116. Within the framework of the intelligence warfighting function, the intelligence tasks and the
1324 intelligence process, intelligence personnel further focus on conducting intelligence from a fundamental
1325 enterprise perspective.

1326 1-117. The Army intelligence enterprise is the sum total of the networked and federated systems, and
1327 efforts of the military intelligence personnel (to include collectors and analysts), sensors, organizations,
1328 information, and processes that allow the focus necessary to use the power of the entire intelligence
1329 community.

1330 1-118. The purpose of the Army intelligence enterprise is to provide technical support and guidance as
1331 well as an information and intelligence architecture that efficiently and effectively synchronize ISR
1332 operations and intelligence analysis and production to drive intelligence production in support of the
1333 commander's situational awareness. Figure 1-2 shows an example of the tactical portion of the Army
1334 intelligence enterprise.

1335

1336

1337

1338

1339

FOR OFFICIAL USE ONLY

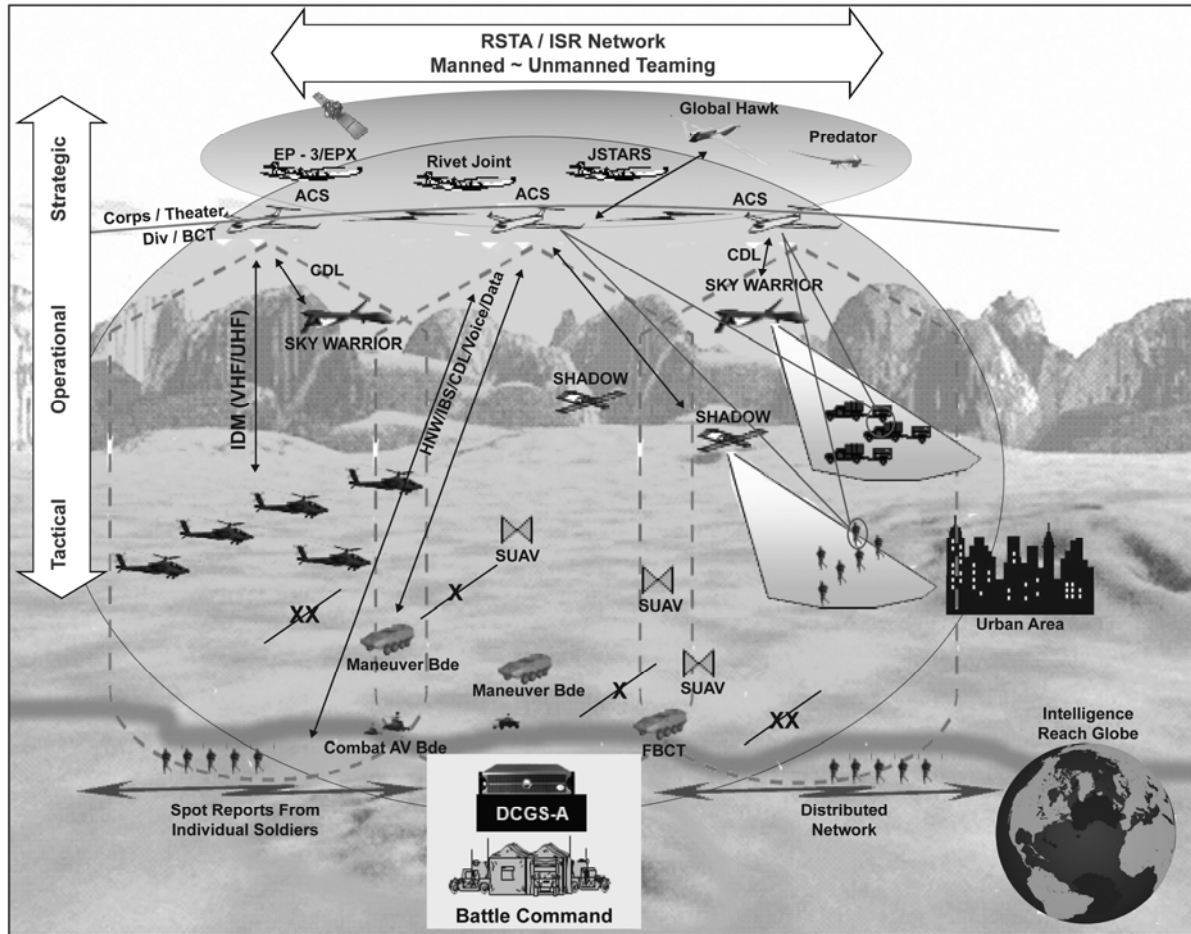


Figure 1-2. Example of the tactical portion of the Army intelligence enterprise

1340
1341

1342 **INTELLIGENCE DISCIPLINES**

1343 1-119. Intelligence is further broken down into disciplines. Each discipline applies unique aspects of
1344 support and guidance called technical channels.

1345 1-120. The Army's intelligence disciplines are all-source intelligence, counterintelligence (CI),
1346 HUMINT, geospatial intelligence (GEOINT), imagery intelligence (IMINT), measurement and signature
1347 intelligence (MASINT), OSINT, SIGINT, and technical intelligence (TECHINT). For more information
1348 regarding the intelligence disciplines, see Part Three of this manual, as well as the respective manuals,
1349 which covers each intelligence discipline.

1350 **ALL-SOURCE INTELLIGENCE**

1351 1-121. All-source intelligence is defined as the intelligence products, organizations, and activities that
1352 incorporate all sources of information and intelligence, including OSINT, in the production of intelligence.
1353 All-source intelligence is a separate intelligence discipline, as well as the name of the step used to produce
1354 intelligence from multiple intelligence or information sources. See chapter 5 for more information on all-
1355 source intelligence.

FOR OFFICIAL USE ONLY

1356 **COUNTERINTELLIGENCE**

1357 1-122. CI counters or neutralizes adversarial, foreign intelligence services, and terrorists (AFIST)
 1358 intelligence collection efforts through collection, CI investigations, operations, analysis, production, and
 1359 functional and technical services. CI includes all actions taken to detect, identify, track, exploit, and
 1360 neutralize the multidiscipline intelligence activities of friends, competitors, opponents, adversaries, and
 1361 enemies; it is the key intelligence community contributor to protect US interests and equities. CI assists in
 1362 identifying essential elements of friendly information, identifying vulnerabilities to threat collection, and
 1363 actions taken to counter collection and operations against US forces. See chapter 6 for more information on
 1364 CI.

1365 **HUMAN INTELLIGENCE**

1366 1-123. HUMINT is the collection of foreign information—by a trained HUMINT collector—from people
 1367 and multimedia to identify elements, intentions, composition, strength, dispositions, tactics, equipment,
 1368 personnel, and capabilities. It uses human sources as a tool and a variety of collection methods, both
 1369 passively and actively, to collect information. See chapter 7 for more information on HUMINT.

1370 **GEOSPATIAL INTELLIGENCE**

1371 1-124. Title 10 US Code § 467 establishes GEOINT. National Geospatial-Intelligence Agency (NGA)
 1372 defines GEOINT as “the exploitation and analysis of imagery and geospatial information to describe,
 1373 assess, and visually depict physical features and geographically referenced activities on the Earth. GEOINT
 1374 consists of imagery, imagery intelligence, and geospatial information.”

1375 1-125. The Army implementation of GEOINT is a result of the Army’s organization, manning, and
 1376 training. There are multiple types of data and information that various Army units and organizations
 1377 collect, provide, and analyze in order to support the GEOINT enterprise. The two primary GEOINT service
 1378 providers in the Army are MI units and organizations and Engineer (topographic) units and organizations:

- 1379 • MI units and organizations provide imagery and IMINT to the enterprise.
- 1380 • Engineer (topographic) units and organizations provide geospatial data and information to the
- 1381 enterprise.
- 1382 • Therefore, while some of the collection, analysis, and exploitation of imagery and geospatial
- 1383 information occur within the intelligence warfighting function; some of the collection, analysis,
- 1384 and exploitation of imagery and geospatial information occur outside the realm of intelligence.
- 1385 See chapter 8 for more information on GEOINT.

1386 1-126. The Army does not conduct GEOINT operations in isolation. GEOINT is comprised of many
 1387 ongoing operations and activities across the DOD. The National System for Geospatial-Intelligence (NSG)
 1388 manages operations through guidance, policy, programs, and organizations. The NSG is the combination of
 1389 technology, policies, capabilities, doctrine, activities, people, data, and communities necessary to produce
 1390 GEOINT in the form of integrated intelligence across multiple environments. The NSG community
 1391 consists of members and partners:

- 1392 • Members include the intelligence community, joint staff, military departments (to include the
- 1393 Services), and combatant commands.
- 1394 • Partners include Civil Applications Committee members, international partners, industry,
- 1395 academia, Defense Service providers, and civil community service providers.

1396 **IMAGERY INTELLIGENCE**

1397 1-127. IMINT is intelligence derived from the exploitation of imagery collected by visual photography,
 1398 infrared, lasers, multi-spectral sensors, and radar. These sensors produce images of objects optically,
 1399 electronically, or digitally on film, electronic display devices, or other media. See chapter 9 for more
 1400 information on IMINT.

FOR OFFICIAL USE ONLY

1401 **MEASUREMENT AND SIGNATURE INTELLIGENCE**

1402 1-128. MASINT is technically derived intelligence that detects, locates, tracks, identifies, and/or
1403 describes the specific characteristics of fixed and dynamic target objects and sources. It also includes the
1404 additional advanced processing and exploitation of data derived from IMINT and SIGINT collection.
1405 MASINT collection systems include but are not limited to radar, spectroradiometric, electro-optical,
1406 acoustic, radio frequency (RF), nuclear detection, and seismic sensors, as well as techniques for collecting
1407 CBRN, and other material samples. See chapter 10 for more information on MASINT.

1408 **OPEN -SOURCE INTELLIGENCE**

1409 1-129. The National Defense Authorization Act for Fiscal Year 2006 states:

1410 *Open source intelligence is produced from publicly available information that is*
1411 *collected, exploited, and disseminated in a timely manner to an appropriate audience for*
1412 *the purpose of addressing a specific intelligence requirement.*

1413 1-130. Expressed in terms of the Army intelligence process, OSINT is relevant information derived from
1414 the systematic collection, processing, and analysis of publicly available information in response to
1415 intelligence requirements.

1416 1-131. The Army does not have a specific military occupational specialty (MOS), additional skill
1417 identifier (ASI), or special qualification identifier (SQI) for OSINT. With the exception of the Asian
1418 Studies Detachment, the Army does not have base tables of organization and equipment (TOE) for OSINT
1419 units or staff elements. OSINT missions and tasks are imbedded within existing missions and force
1420 structure or accomplished through task organization. See chapter 11 for more information on OSINT.

1421 **SIGNALS INTELLIGENCE**

1422 1-132. SIGINT is intelligence produced by exploiting foreign communication systems and
1423 noncommunications emitters. SIGINT provides unique intelligence and analysis information in a timely
1424 manner. The discipline is comprised of communications intelligence (COMINT), electronic intelligence
1425 (ELINT), and foreign instrumentation signals intelligence (FISINT). See chapter 12 for more information
1426 on SIGINT.

1427 **TECHNICAL INTELLIGENCE**

1428 1-133. TECHINT is intelligence derived from the collection and analysis of threat and foreign military
1429 equipment and associated materiel for the purposes of preventing technological surprise, assessing foreign
1430 scientific and technical capabilities, and developing countermeasures designed to neutralize an adversary's
1431 technological advantages. See chapter 13 for more information on TECHINT.

1432 **EMERGING CAPABILITIES**

1433 1-134. Four emerging capabilities which are not intelligence-specific capabilities, but which will impact
1434 intelligence operations, are biometrics, DCGS-A, human terrain analysis teams, and document and media
1435 exploitation (DOMEX).

1436 **BIOMETRICS**

1437 1-135. A biometric is defined by JP 2-0 as a measurable physical characteristic or personal behavioral
1438 trait used to recognize the identity or verify the claimed identity of an individual. **Biometrics-enabled**
1439 **intelligence is defined as the intelligence information associated with biometrics data that matches a**
1440 **specific person or unknown identity to a place, activity, device, component, or weapon that supports**
1441 **terrorist or insurgent networks and related pattern analysis; facilitates high-value individual**
1442 **targeting; reveals movement patterns; and confirm identities (DOD Directive 8521).**

FOR OFFICIAL USE ONLY

- 1443 1-136. Typical automated biometric systems are comprised of five integrated components:
- 1444 ● **Collection Device.** Hardware found on a biometric device that converts biometric input into a
- 1445 digital signal and conveys this information to the processing device.
- 1446 ● **Algorithms.** A sequence of instructions that tells a biometric system how to solve a particular
- 1447 problem. An algorithm will have a finite number of steps and is typically used by the biometric
- 1448 engine to compute whether a match exists between a biometric sample and a biometric template.
- 1449 ● **Database.** Used to store the information collected that will be used later to do matching against.
- 1450 ● **Decision Process.** Automated or human-assisted process or analysis that results in a decision by
- 1451 matching components and specific search criteria.
- 1452 ● **Dissemination Process.** Gets the data collected to whomever and wherever it needs to be in a
- 1453 timely manner.
- 1454 1-137. The implementation of these five components leads to personal identification (PI) or the
- 1455 identification of an individual with certitude. This can be summarized into three stages:
- 1456 ● The sensor collects a biometric feature to include fingerprints, iris, or photographic image of
- 1457 face, or DNA.
- 1458 ● The system stores that feature in a mathematical template in a database.
- 1459 ● The processing device runs search on the template against a matching algorithm that compares it
- 1460 to templates already stored in the database.
- 1461 1-138. Military commanders require the ability to link identity information to a given individual.
- 1462 Biometric systems are employed to deny threat forces freedom of movement within the populace and
- 1463 positively identify known threats. These systems gather biometric data such as iris scans, fingerprints, and
- 1464 photographic images and combine them with contextual data to produce an electronic dossier on the
- 1465 individual.
- 1466 1-139. PI includes positively identifying friendly, adversarial, non-adversarial forces. Intelligence-
- 1467 related functions that biometrics can support or enhance are—
- 1468 ● Intelligence analysis.
- 1469 ● Foreign national and local employee hires screening.
- 1470 ● Counterintelligence and force protection (FP).
- 1471 ● Interrogation and detention operations.
- 1472 ● HVT confirmation (including high-value individuals [HVIs] and killed in action).
- 1473 ● Base access and local security.
- 1474 ● Population control or census (screening, enrolling, and badging operations).
- 1475 1-140. The capability to positively identify an individual and to place that individual within a relevant
- 1476 context adds a level of certitude that significantly enhances the overall effectiveness of the mission. PI
- 1477 enabled by biometric technology can help to identify and locate specific individuals in support of targeting.
- 1478 This capability is necessary not only for FP and security missions but also when an operational capability is
- 1479 required to achieve an advantage over an enemy in conventional warfare, combating terrorism, forcible
- 1480 entry, strikes, raids, and operations with multinational partners.
- 1481 1-141. Affixing an individual's identification using the person's unique physical features and linking this
- 1482 identity to the individual's past activities and previously used identities such as friendly forces' accesses,
- 1483 permissions, clearance status, medical information, and unique biometrically based identifiers, in addition
- 1484 to adversary or unknown persons. Ensuring access to all available information on an individual is critical to
- 1485 such functions as screening persons for access to vessels, position of trust, and the prosecution of criminals
- 1486 and terrorists. As biometric capabilities continue to develop and current operations change in nature, it is
- 1487 necessary to integrate the operational, intelligence, and communications aspects of biometrics systems into
- 1488 a cohesive concept of employment.
- 1489 1-142. For more information on biometrics enabled intelligence, see TC 2-22,101 when published.

FOR OFFICIAL USE ONLY

1490 **DISTRIBUTED COMMON GROUND SYSTEM-ARMY**

1491 1-143. DCGS-A provides a net-centric, enterprised ISR, weather, geospatial engineering, and space
1492 operations capability to maneuver, maneuver support, and maneuver sustainment support organizations at
1493 all echelons from the battalion to JTFs. DCGS-A will be the ISR component of the modular and future
1494 force Battle Command System and the Army’s primary system for ISR tasking, posting, processing, and
1495 using information about the threat, terrain, weather, and civil considerations at all echelons.

1496 1-144. DCGS-A provides the capabilities necessary for commanders to access information from all data
1497 sources and to synchronize sensors. DCGS-A provides continuous acquisition and synthesis of data and
1498 information from joint and interagency capabilities, multinational partners, and non-traditional sources that
1499 will permit forces to maintain an updated and accurate understanding of the operational environment.
1500 DCGS-A contributes to visualization and situational awareness, thereby enhancing tactical maneuver,
1501 maximizing combat power, and enhancing the ability to operate in an unpredictable and changing
1502 operational environment throughout full spectrum operations.

1503 1-145. DCGS-A will facilitate the rapid conduct of operations and synchronization of all warfighting
1504 functions resulting in the ability to operate within the threat’s decision cycle, as well as to shape the
1505 environment for successful operations. The core functions of DCGS-A are—

- 1506 ● Receipt and processing of select ISR sensor data.
- 1507 ● Control of select Army sensor systems.
- 1508 ● Facilitation of ISR synchronization.
- 1509 ● Facilitation of ISR integration.
- 1510 ● Fusion of sensor information.
- 1511 ● Direction and distribution of relevant threat.
- 1512 ● Facilitation of friendly and environmental (weather and terrain) information.

1513 **HUMAN TERRAIN ANALYSIS TEAMS**

1514 1-146. A headquarters may request a human terrain analysis team to assist with socio-cultural research
1515 and analysis. As part of building their situational understanding, commanders consider how culture (both
1516 their own and others within the AO) affects operations. Culture is examined as part of the mission variable
1517 civil considerations. Understanding the culture of a particular society or group within a society
1518 significantly improves the force’s ability to accomplish the mission. Army leaders are mindful of cultural
1519 factors in three contexts:

- 1520 ● Sensitivity to the different backgrounds of team members to best leverage their talents.
- 1521 ● Awareness of the culture of the country in which the organization operates.
- 1522 ● Consideration of the possible implication of partners’ customs, traditions, doctrinal principles,
1523 and operational methods when working with their forces.

1524 1-147. Effective Army leaders understand and appreciate their own culture (individual, military, and
1525 national) in relationship to the various cultures of others in the AO. Just as culture shapes how other groups
1526 view themselves and the world around them, culture shapes how commanders, leaders, and Soldiers
1527 perceive the world. Effective commanders are aware that their individual perceptions greatly influence how
1528 they understand the situation and make decisions. Through reflection, dialog, engagement, and analysis of
1529 differences between their culture and that of the indigenous population, commanders expose and question
1530 their assumptions about situation. They seek to understand how enemies, partners, and the population view
1531 the situation.

1532 **DOCUMENT AND MEDIA EXPLOITATION IN MODERN MILITARY OPERATIONS**

1533 1-148. Modern military operations are conducted in volatile, complex, and ever-changing operational
1534 environments. It is essential for tactical military leaders to have access to accurate and timely information

FOR OFFICIAL USE ONLY

1535 when planning and conducting operations. Tactical, operational, and strategic leaders are enabled with
 1536 accurate information about enemy forces through the rapid and accurate extraction, exploitation, and
 1537 analysis of captured enemy documents (CEDs), media, and materiel.

1538 1-149. DOMEX is the systematic extraction of information from all media in response to the
 1539 commander's collection requirements. When conducted properly, DOMEX operations are intended to—

- 1540 ● Maximize the value of intelligence gained from captured enemy documents and media.
- 1541 ● Provide the commander with timely and relevant intelligence to effectively enhance awareness
 1542 of the enemy's capabilities, operational structures, and intent.
- 1543 ● Provide timely and accurate intelligence support to the warfighter throughout the entire range of
 1544 military operations.
- 1545 ● Assist in criminal prosecution or legal processes by maintaining chain of custody procedures
 1546 and preserving the evidentiary value of captured materials.

1547 1-150. As an integral part of today's operational environment, DOMEX is an increasingly specialized
 1548 full-time mission requiring advanced automation and communications support, analytical support, and
 1549 expert linguists. DOMEX and translation operations were once considered purely HUMINT processing
 1550 activities directly associated with language capabilities and extensive background knowledge in area
 1551 studies.

1552 1-151. Current doctrinal thought acknowledges that HUMINT is no longer the sole asset capable of
 1553 conducting DOMEX operations. Personnel involved in DOMEX do not require HUMINT training in order
 1554 to screen or translate a document, particularly since the unit may better utilize its sparse HUMINT assets to
 1555 conduct the HUMINT mission. DOMEX is an Armywide responsibility and while HUMINT assets may be
 1556 utilized to perform the DOMEX mission when available, HUMINT is a consumer of DOMEX information,
 1557 rather than the major provider.

1558 1-152. For DOMEX products to be a force multiplier, the rapid exploitation of captured materials must
 1559 occur at the lowest echelon possible. DOMEX assets pushed down to the tactical level provide timely and
 1560 accurate intelligence support to the warfighter; not only does this enable the rapid exploitation and
 1561 evacuation of captured materials, it also hastens the feedback commanders receive from the higher-echelon
 1562 analysis of captured materials affecting operations.

1563 1-153. The current methodology for intelligence dissemination sends reporting through an echeloned
 1564 structure from national, to theater, to corps, to division, and so on, then back down through the same rigid
 1565 structure. Recent military operations have shown that this methodology is not timely and seldom results in
 1566 lower tactical echelons receiving intelligence critical to their AO. The intelligence staff must be prepared to
 1567 use any form of communication to pass vital information.

1568 1-154. Depending upon the tactical situation, available resources, and the CCIRs, PIRs, SIRs, critical
 1569 pieces of information must be passed quickly to those who can use them; specifically, tactical commanders.
 1570 Intelligence staffs are responsible for reporting and disseminating DOMEX-derived information in a
 1571 manner that ensures the information reaches not only the next higher echelon but also the tactical
 1572 commander most affected by the information.

1573 1-155. In today's operational environment, commanders and staff must determine how to task-organize
 1574 their ISR units to best satisfy their information requirements. Additionally, commanders anticipating
 1575 requirements their unit cannot satisfy must consider requesting specialized or uniquely trained units.
 1576 Assigning these units to the requesting organization may be the best solution, but often specialized units
 1577 are allocated to higher headquarters and are attached to requesting units based on availability and priority.

1578 1-156. In addition to identifying information requirements and capable ISR units, planning to conduct
 1579 DOMEX operations efficiently requires a synchronized concept of operations. Other than intelligence
 1580 units, assigned intelligence personnel representation generally ends at the battalion echelon with the
 1581 battalion intelligence staff. Battalion staffs must plan for DOMEX operations from their subordinate units.
 1582 Two techniques to provide better intelligence below the battalion echelon are to task-organize intelligence

FOR OFFICIAL USE ONLY

1583 personnel as intelligence support teams to company or platoon echelon, or to train company or platoon
1584 personnel in specific handling, screening, and inventorying techniques.

1585 1-157. Where tactical assets are insufficient, operational and strategic assets can be relied upon to support
1586 a unit's organic assets, either via personnel augmentation or via virtual or long-distance support to tactical
1587 operations from continental United States and outside continental United States DOMEX support elements
1588 worldwide.

1589 1-158. The skills, knowledge, and equipment for specialized processing are available at intelligence
1590 community organizations through the communications architecture. Units can request the National Security
1591 Agency (NSA), the Defense Intelligence Agency (DIA), the National Geospatial-Intelligence Agency
1592 (NGA), the National Media Exploitation Center (NMEC), the National Ground Intelligence Center
1593 (NGIC), the Joint Document Exploitation Center (JDEC), and other US or multinational intelligence
1594 community organizations to use specialized techniques and procedures to extract additional information
1595 from captured audio and video materials. Application of specialized processing techniques and procedures
1596 may require the classification of the processed information and restrict its dissemination.

FINAL DRAFT

FOR OFFICIAL USE ONLY

1597

Chapter 2

1598

Intelligence Communities and Joint Considerations

1599 2-1. *Unified action is the synchronization, coordination, and/or integration of the activities of*
1600 *governmental and nongovernmental entities with military operations to achieve unity of effort (JP 1).*
1601 Under unified action, commanders integrate joint, single-service, special, and supporting intelligence
1602 operations with interagency, nongovernmental, and multinational operations. Army Forces (ARFOR) often
1603 bring unique ISR capabilities to unified action.

1604 2-2. This chapter discusses the synchronization of Army intelligence efforts with joint and other national
1605 and international partners to achieve unity of effort and to accomplish the commander's intent.

1606

INTELLIGENCE COMMUNITY

1607 2-3. There are many organizations in the intelligence community that support military operations by
1608 providing specific intelligence products and services. The J-2/G-2/S-2 and the staff must be familiar with
1609 these organizations and the methods of obtaining information from them as necessary. Figure 2-1 shows
1610 organizations that compose the intelligence community.

1611

DOD AGENCIES

1612 2-4. The DOD agencies are discussed below.

1613

Defense Intelligence Agency

1614 2-5. The Defense Intelligence Agency (DIA) has oversight of the Defense Intelligence Analysis Program
1615 and provides intelligence support in areas, such as all-source military analysis, human factors analysis,
1616 HUMINT, MASINT, Medical Intelligence, CI, counterterrorism, chemical, biological, radiological,
1617 nuclear, and high yield explosives (CBRNE) counterproliferation, counterdrug operations, information
1618 operations, personnel recovery, peacekeeping and multinational support, noncombatant evacuation
1619 operations, I&W, targeting, battle damage assessment (BDA), current intelligence, systems analysis of the
1620 adversary, collection management, intelligence architecture and systems support, intelligence support to
1621 operation planning, defense critical infrastructure protection, and document and media exploitation
1622 (DOMEX).

1623

National Security Agency/Central Security Service

1624 2-6. The National Security Agency/Central Security Service is a unified organization structured to
1625 provide for the SIGINT mission of the US and to ensure the protection of national security systems for all
1626 departments and agencies of the US Government.

1627

National Geospatial-Intelligence Agency

1628 2-7. NGA provides timely, relevant, and accurate GEOINT support to include IMINT, GEOINT,
1629 national imagery collection management, commercial imagery, imagery-derived MASINT, and some
1630 meteorological and oceanographic data and information.

FOR OFFICIAL USE ONLY

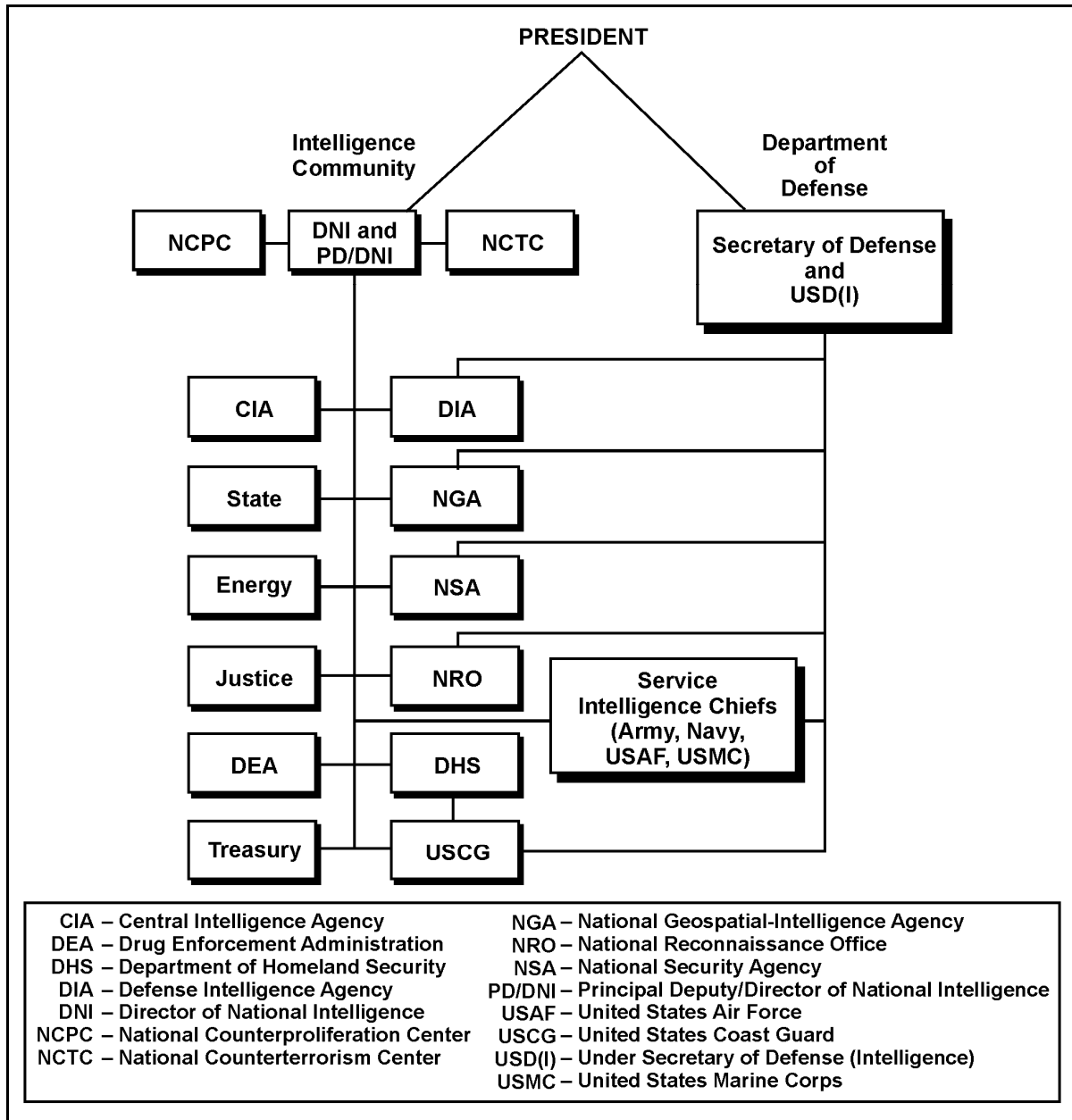


Figure 2-1. Intelligence community membership

1631

1632 National Reconnaissance Office

1633 2-8. The National Reconnaissance Office (NRO) is responsible for integrating unique and innovative
 1634 space-based reconnaissance technologies, and the engineering, development, acquisition, and operation of
 1635 space reconnaissance systems and related intelligence activities.

FOR OFFICIAL USE ONLY

1636 **Joint Reserve Intelligence Centers**

1637 2-9. A Joint Reserve Intelligence Center (JRIC) is a joint intelligence production and training activity that
 1638 uses information networks to link reservist intelligence personnel with the combatant commands and
 1639 Services. A JRIC is located within a Service-owned and managed sensitive compartmented information
 1640 facility (SCIF) and may also include surrounding collateral and unclassified areas involved in the
 1641 performance and direct management of intelligence production work that uses Joint Reserve Intelligence
 1642 Program infrastructure and connectivity. The more than 20 JRICs located around the country are equipped
 1643 to effectively serve as satellite elements to combatant command JIOCs. JRICs are shared facilities that
 1644 serve multiple customers and missions (JP 2-0).

1645 **US Army Intelligence**

1646 2-10. The Army Deputy Chief of Staff (DCS) for Intelligence exercises staff supervision over the US
 1647 Army Intelligence and Security Command (INSCOM).

1648 *US Army Intelligence and Security Command*

1649 2-11. INSCOM, which includes the National Ground Intelligence Center, provides intelligence support to
 1650 strategic and operational level commanders in the areas of IMINT, MASINT, SIGINT, operational and
 1651 tactical HUMINT, CI, TECHINT, information operations, general military intelligence (GMI), and
 1652 scientific and technical intelligence (S&TI). Other organizations include the Army Reserve Military
 1653 Intelligence Readiness Command.

1654 2-12. The US Army has vested its intelligence at the operational level with INSCOM, a direct reporting
 1655 unit responsible for the Army's intelligence forces above corps. INSCOM's mission is to conduct and
 1656 support intelligence, security, and information operations for military commanders and national decision
 1657 makers. INSCOM goal is to provide superior information and information capabilities to Army
 1658 commanders, while denying the same to adversaries. Headquarters, INSCOM, in coordination with its
 1659 major subordinate commands (MSCs), provides a myriad of general intelligence support operations.
 1660 INSCOM serves as the national to tactical intelligence conduit.

1661 *Army Space Program Office*

1662 2-13. The Army Space Program Office (ASPO) executes the Army's Tactical Exploitation of National
 1663 Capabilities Program (TENCAP). The program focuses on exploiting current and future tactical potential
 1664 of national systems and integrating the capabilities into the Army's tactical decision-making process. Army
 1665 TENCAP systems enable the tactical commander maximum flexibility to satisfy intelligence needs under a
 1666 wide range of operational scenarios. ASPO is the point of contact (POC) for all tactical activities between
 1667 direct reporting units or users and the NRO.

1668 **US Navy Intelligence**

1669 2-14. The Director of Naval Intelligence exercises staff supervision over the Office of Naval Intelligence,
 1670 which provides the intelligence necessary to plan, build, train, equip, and maintain US naval forces. The
 1671 National Maritime Intelligence Center consists of Office of Naval Intelligence, the US Coast Guard
 1672 Intelligence Coordination Center, the Navy Information Operations Command, and detachments of the
 1673 Marine Corps Intelligence Activity and Naval Criminal Investigative Service.

1674 **US Air Force Intelligence**

1675 2-15. The Air Force DCS for Intelligence, Surveillance, and Reconnaissance is responsible for intelligence
 1676 policy, planning, programming, evaluation, and resource allocation. The Air Force's main production
 1677 facility is the National Air and Space Intelligence Center. Primary collection, analysis, and production units
 1678 are organized under the Air Combat Command, the Air Force Warfare Center, and the Air Force
 1679 Intelligence, Surveillance, and Reconnaissance Agency. Additionally, the Air Force Office of Special

FOR OFFICIAL USE ONLY

1680 Investigations is the Service's main focal point for CI activities. Additional information describing the Air
1681 Force approach to operational ISR employment is found in AFDD 2-9.

1682 **US Marine Corps Intelligence**

1683 2-16. The Director of Intelligence is the Commandant's principal intelligence staff officer and the
1684 functional manager for intelligence, CI, and cryptologic material. The Director exercises staff supervision
1685 of the Marine Corps Intelligence Activity, which provides tailored intelligence products to support Marine
1686 Corps operating forces, and serves as the fixed site of the Marine Corps Intelligence Surveillance and
1687 Reconnaissance Enterprise.

1688 **NONMILITARY MEMBERS OF THE INTELLIGENCE COMMUNITY**

1689 2-17. Joint operations require knowledge of both military and nonmilitary aspects of the operational
1690 environment. Much of this expertise falls outside the purview of the DOD members of the intelligence
1691 community. JFCs and their J-2's should be familiar with the roles and responsibilities of the following non-
1692 DOD members of the intelligence community.

1693 **Director of National Intelligence**

1694 2-18. The office of the Director of National Intelligence oversees the Intelligence Community
1695 organizations; leads the national intelligence effort.

1696 **Central Intelligence Agency**

1697 2-19. The Central Intelligence Agency's (CIA) primary areas of expertise are in HUMINT collection, all-
1698 source analysis, and the production of political, economic, and biographic intelligence.

1699 **Department of State**

1700 2-20. The Department of State's Bureau of Intelligence and Research performs intelligence analysis and
1701 production on a wide range of political and economic topics essential to foreign policy determination and
1702 execution.

1703 **Department of Energy**

1704 2-21. The Department of Energy analyzes foreign information relevant to US energy policies and
1705 nonproliferation issues.

1706 **Federal Bureau of Investigation**

1707 2-22. The Federal Bureau of Investigation has primary responsibility for CI and CT operations conducted
1708 in the US. The Federal Bureau of Investigation shares law enforcement and CI information with
1709 appropriate DOD entities and combatant commands.

1710 **Department of the Treasury**

1711 2-23. The Department of the Treasury analyzes foreign intelligence related to economic policy and
1712 participates with the Department of State in the overt collection of general foreign economic information.

1713 **United States Coast Guard**

1714 2-24. The US Coast Guard operates as both a military service and a law enforcement organization and
1715 provides general maritime intelligence support to commanders from the strategic to tactical level in the
1716 areas of HUMINT, SIGINT, GEOINT, MASINT, OSINT, and CI.

FOR OFFICIAL USE ONLY

1717 **Department of Homeland Security**

1718 2-25. The Directorate for Information Analysis and Infrastructure Protection analyzes the vulnerabilities of
1719 US critical infrastructure, assesses the scope of terrorist threats to the US homeland, and provides input to
1720 the Homeland Security Advisory System.

1721 **Drug Enforcement Administration**

1722 2-26. The Office of National Security Intelligence collects and analyzes information related to illegal drug
1723 production, smuggling, and trafficking.

1724 **OTHER AGENCIES**

1725 2-27. There are a number of US Government agencies and organizations, not members of the intelligence
1726 community, that are responsible for collecting and maintaining information and statistics related to foreign
1727 governments and international affairs. Organizations such as the Library of Congress, the Departments of
1728 Agriculture and Commerce, the National Technical Information Center, and the US Patent Office are
1729 potential sources of specialized information on political, economic, and military-related topics. The
1730 intelligence community may draw on these organizations to support and enhance research and analysis and
1731 to provide relevant information and intelligence for commanders and planners.

1732 2-28. Many other US Government agencies may become directly involved in supporting DOD especially
1733 during stability operations. (See JP 2-02 for a description of agency support to joint operations and
1734 intelligence.) These organizations include—

- 1735 ● Department of Transportation.
- 1736 ● Disaster Assistance Response Team within the Office of Foreign Disaster.
- 1737 ● US Agency for International Development.

1738 **THE LEVELS OF WAR**

1739 2-29. The levels of war are doctrinal perspectives that define and clarify the relationship between strategy,
1740 operational approach, and tactical actions. Although there are no finite limits or boundaries between them,
1741 the three levels of war are strategic, operational, and tactical (see figure 2-2).

- 1742 ● The strategic level is that level at which a nation, often as a member of a group of nations,
1743 determines national or multinational (alliance or coalition) strategic security objectives and
1744 guidance, and develops and uses national resources to achieve these objectives.
- 1745 ● The operational level links employing tactical forces to achieving the strategic end-state. At the
1746 operational level, commanders conduct campaigns and major operations to establish conditions
1747 that define that end-state.
- 1748 ● The tactical level is the employment and ordered arrangement of forces in relation to each other
1749 (CJCS Instruction 5120.02A). Through tactics, commanders use combat power to accomplish
1750 missions. The tactical level commander uses combat power in battles, engagements, and small-
1751 unit actions.

FOR OFFICIAL USE ONLY

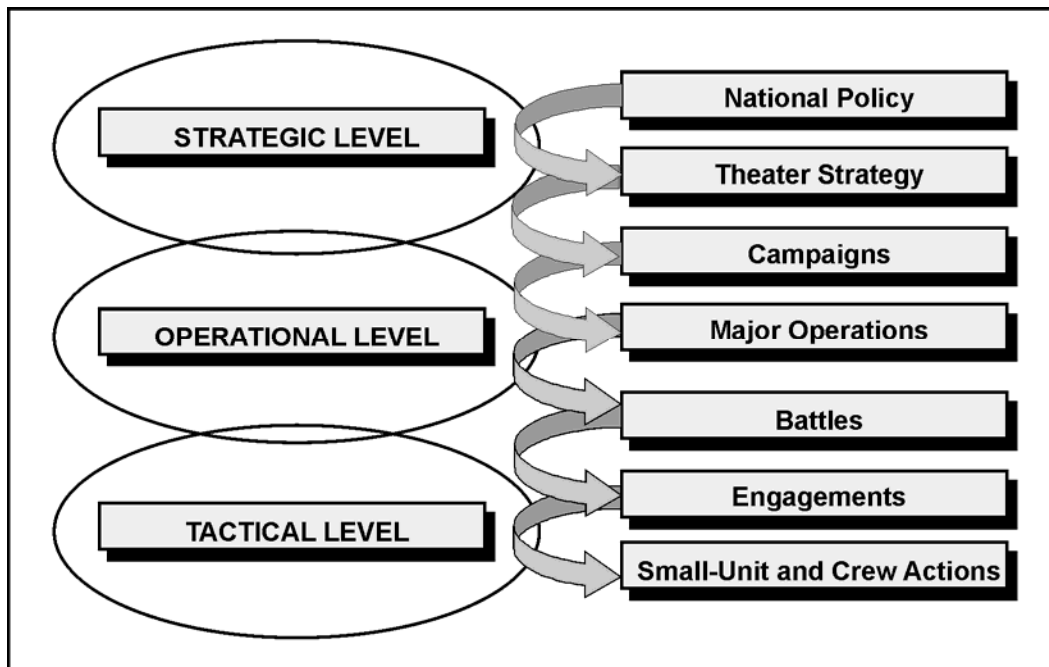


Figure 2-2. Levels of war

1752

1753 2-30. Understanding the interdependent relationship of all three levels of war helps commanders visualize
 1754 a logical flow of operations, allocate resources, and assign tasks. Actions within the three levels are not
 1755 associated with a particular command level, unit size, equipment type, or force or component type. The
 1756 concept of strategic, operational, and tactical intelligence operations commanders and their intelligence
 1757 officers in visualizing the flow of intelligence from one level to the next. The concept facilitates allocating
 1758 required collection, analysis, production, and dissemination resources; and facilitates the assignment of
 1759 appropriate intelligence tasks to national, combatant command, component, and supporting intelligence
 1760 elements.

1761 STRATEGIC

1762 2-31. The President and the Secretary of Defense use strategic intelligence to develop national strategy and
 1763 policy, monitor the international situation, prepare military plans, determine major weapon systems and
 1764 force structure requirements, and conduct strategic operations

1765 2-32. Intelligence supports joint operations across the full spectrum of military operations. It determines
 1766 the current capabilities, and forecasts future developments, threats that could affect the national security
 1767 and interests. During strategic operations, intelligence personnel also produce the intelligence required by
 1768 CCDRs to prepare strategic estimates, strategies, and plans to accomplish missions assigned by higher
 1769 authorities.

1770 2-33. Combatant command intelligence includes determining when, where, and in what strength the threat
 1771 will stage and conduct combatant command level campaigns and strategic unified operations. The
 1772 intelligence staff should also focus predictive analysis efforts on identifying strategic threat events and how
 1773 these events will impact US actions at the strategic, operational, and tactical levels. Intelligence operations
 1774 support information operations as well. Intelligence operations support strategic planning by—

- 1775 ● Developing strategic intelligence policy.
- 1776 ● Preparing the strategic collection plan.

FOR OFFICIAL USE ONLY

- 1777 • Allocating national intelligence resources.
- 1778 2-34. Collection on intelligence requirements can provide information which identifies indicators of threat
 1779 actions or intent, thus reducing the uncertainties associated with an operation. Significant changes (that is,
 1780 branches and sequels) during or to an operation usually lead to changes in intelligence requirements. Of
 1781 particular importance is information relating to threat strategic vulnerabilities, strategic forces, strategic
 1782 centers of gravity (COGs), and any capabilities relating to the development and employment of CBRNE
 1783 weapons.
- 1784 2-35. Global and regional issues and threats are identified and reported to the President and the Secretary
 1785 of Defense, as well as to the senior military leadership and the CCDR. Intelligence requirements include
 1786 any foreign developments that could threaten the US, its citizens abroad, or multinational military,
 1787 political, or economic interests. Intelligence also includes identifying hostile reactions to US
 1788 reconnaissance activities and indications and warnings (I&W) of impending terrorist attacks.

1789 **OPERATIONAL**

- 1790 2-36. CCDRs and subordinate JFCs and their component commanders are the primary users of operational
 1791 intelligence. At the operational echelons, intelligence—
- 1792 • Focuses on the military capabilities and intentions of threats.
 - 1793 • Provides analysis of events within the AOI and helps commanders determine when, where, and
 1794 in what strength the adversary might stage and conduct campaigns and major operations.
 - 1795 • Supports all phases of military operations, from mobilization through general war to stable
 1796 peace and all the way through redeployment of US forces. It continues during sustainment.
 - 1797 • Supports all aspects of the joint campaign.
 - 1798 • Identifies adversary COGs and HVTs.
 - 1799 • Provides critical support to friendly information tasks.
- 1800 2-37. The JFC and staff allocate intelligence resources and request support from national agencies, other
 1801 combatant commands, and multinational partners. During stability operations, operational intelligence
 1802 includes training and assisting multinational partners in conducting intelligence operations.
- 1803 2-38. CCDRs use intelligence concerning the factors of the operational environment to determine the type
 1804 and scale of operations.
- 1805 2-39. Intelligence also aids in determining the impact of significant regional features and hazards on the
 1806 conduct of both friendly and threat operations. Significant regional factors include the civil considerations
 1807 applied to the AOI. Intelligence analysis also assists in recommending the rules of engagement (ROE) and
 1808 other restrictions which will affect operations in the JFC's JOA.
- 1809 2-40. Intelligence relating to the threat's military and nonmilitary capabilities assists in determining the
 1810 threat's ability to conduct military operations. Factors that operational intelligence addresses include
 1811 mobilization potential, force structure (including alliance forces), force dispositions, equipment, doctrine,
 1812 C2 structure, goals, and their decision-making process. Intelligence includes the continuous refinement of
 1813 the threat characteristics for the entire array of the enemy's forces in the AOI.

1814 **TACTICAL**

- 1815 2-41. Timely, relevant, accurate, predictive, and tailored intelligence allows tactical units to achieve an
 1816 advantage over the threat and is essential for mission success. Predictive intelligence also enables the staff
 1817 to better develop COAs. Tactical intelligence—
- 1818 • Identifies and assesses the threat's tactical capabilities, COAs, and vulnerabilities, as well as
 1819 describes AO.
 - 1820 • Seeks to identify when, where, and in what strength the enemy will conduct operations.

FOR OFFICIAL USE ONLY

- 1821 ● Provides the commander with information on imminent threats to the force including those from
- 1822 terrorists, saboteurs, insurgents, and foreign intelligence collection.
- 1823 ● Provides critical support to friendly information tasks.
- 1824 ● Develops and disseminates targeting information and intelligence.

1825 2-42. Intelligence provides the tactical commander with the information and intelligence required to

1826 conduct missions against threat forces. At the tactical level, the intelligence tasks support the execution of

1827 battles and engagements. These intelligence tasks have a different focus than those at other levels due to

1828 their ability to immediately influence the outcome of the tactical commander's mission. They include

1829 information gathered from tactical sources, such as combat information, interrogations, debriefings, and

1830 eliciting information from captured or misplaced personnel. For a complete listing of tactical collective

1831 tasks, refer to FM 7-15.

1832 INTELLIGENCE REACH

1833 2-43. The G-2/S-2 must determine how best to support the unit's mission with intelligence reach

1834 capabilities. Detailed planning and training are critical to the success of intelligence reach operations.

1835 Intelligence reach supports distributed analysis in support of the CCIR. Table 2-1 shows examples of

1836 partners and sources for intelligence reach. The following are steps that the staff can take to ensure optimal

1837 use, operability, and effectiveness of intelligence reach:

- 1838 ● Establish data exchange methods and procedures.
- 1839 ● Establish electronic message transfer procedures.
- 1840 ● Establish homepages for identified forces.
- 1841 ● Establish POCs for I&W centers, production centers, combatant command Joint Intelligence
- 1842 Operations Centers (JIOC), DIA, INSCOM, and their MSCs, such as National Ground
- 1843 Intelligence Center (NGIC) and the higher MI organizations.
- 1844 ● Ensure the intelligence staff has the necessary personnel, training, automated systems,
- 1845 bandwidth, and resources to conduct intelligence reach.
- 1846 ● Determine IRs through staff planning. Develop production requirements for identified
- 1847 intelligence gaps.
- 1848 ● Order geospatial products for the projected AOI.
- 1849 ● Establish and maintain a comprehensive directory of intelligence reach resources before
- 1850 deployment and throughout operations. The value of intelligence reach will greatly increase as
- 1851 the staff develops and maintains ready access to rich information resources. These resources are
- 1852 numerous and may include, for example, Army, Joint, DOD, non-DOD, national, commercial,
- 1853 foreign, and university research programs.
- 1854 ● Know what types of information the resources can provide. Continuously expand the resource
- 1855 directory through identification of new resources.
- 1856 ● Use intelligence reach first to fill intelligence gaps and requirements and answer RFIs. This
- 1857 technique can preclude unnecessary tasking or risk to limited ISR assets.
- 1858 ● Maintain continuous situational understanding and anticipate intelligence requirements. Use
- 1859 intelligence reach to fulfill these requirements and provide the results to the commander and
- 1860 staff for the conduct of operations.
- 1861 ● Exchange intelligence reach strategies with other units.
- 1862 ● Present the information retrieved through intelligence reach in a usable form. Share the
- 1863 information derived from intelligence reach with subordinate, lateral, and higher echelons.
- 1864 Ensure follow-on forces have all information as well.

1865 CATEGORIES OF INTELLIGENCE PRODUCTS

1866 2-44. Intelligence products are generally placed in one of seven production categories:

FOR OFFICIAL USE ONLY

- 1867 ● I&W.
- 1868 ● Current intelligence.
- 1869 ● GMI.
- 1870 ● Target intelligence.
- 1871 ● S&TI.
- 1872 ● CI.
- 1873 ● Estimative.

1874 2-45. The categories of intelligence are distinguishable from each other primarily by the purpose of the
 1875 intelligence product. The categories can overlap and some of the same intelligence is useful in more than
 1876 one category. Depending upon the echelon, intelligence organizations use specialized procedures to
 1877 develop each category of intelligence. The following information describes each category.

Table 2-1. Examples of partners and sources for intelligence reach

ARMY	SERVICES	JOINT	DOD
ACE ISE MIB 902d NGIC ATCAE ARISCs USAIC Cultural Center USACHCS World Religion Center	ONI NMIC AF ISR Agency NASIC MCIA	USEUCOM JAC USSOUTHCOM JIOC USSOCOM JIOC USSPACECOM CIC USJFCOM AIC USCENTCOM JIOC USTRANSCOM JIOC USSTRATCOM USPACOM JOIC USNORTHCOM JIOC USAFRICOM JIOC	DIA CMO MSIC NCMI DAO DH NGA NSA RSOCs
NON-DOD	NATIONAL	COMMERCIAL	FOREIGN
DOE FBI DOS DEA FEMA ICE	DNI NIC CIA NRO INR DOT, Office of Intel Support DHS	RAND Jane's Defense Weekly Economic Intelligence Unit CNN Reuters Associated Press United Press International	DIS NDHQ DIO

1879 **INDICATIONS AND WARNINGS**

1880 2-46. I&W are those intelligence activities intended to detect and report time-sensitive intelligence
 1881 information on foreign developments that could pose a threat to the US or multinational military, political,
 1882 or economic interests or to US citizens abroad. I&W includes forewarning of threat actions or intentions;
 1883 the imminence of hostilities; insurgency; nuclear or non-nuclear attack on the US, US overseas forces, or
 1884 multinational forces; hostile reactions to US reconnaissance activities; terrorist attacks; and other similar
 1885 events. (See JP 2-0 for more information on I&W.)

1886 2-47. While the G-2/S-2 is primarily responsible for producing I&W intelligence, each element, such as
 1887 the MP conducting PIO, within every unit contributes to I&W through awareness of the CCIRs and
 1888 reporting related information.

1889 **CURRENT INTELLIGENCE**

1890 2-48. Current intelligence involves the integration of time-sensitive, all-source intelligence and
 1891 information into concise, accurate, and objective reporting on the AO and current threat situation. One of

FOR OFFICIAL USE ONLY

1892 the most important forms of current intelligence is the threat situation portion of the COP. The
1893 G-2/S-2 is responsible for producing current intelligence for the unit. Current intelligence supports ongoing
1894 operations during the full spectrum of operations. In addition to the current situation, current intelligence
1895 should provide projections of the threat's anticipated situations (estimates) and their implications on the
1896 friendly operation. (See JP 2-0.)

1897 **GENERAL MILITARY INTELLIGENCE**

1898 2-49. GMI is intelligence concerning military capabilities of foreign countries or organizations or topics
1899 affecting potential US or multinational military operations relating to armed forces capabilities, including
1900 threat characteristics, organization, training, tactics, doctrine, strategy, and other factors bearing on military
1901 strength and effectiveness and area and terrain intelligence. This broad category of intelligence is normally
1902 associated with long-term planning at the national level. However, GMI is also an essential tool for the
1903 intelligence staff and should be in place long before the start of preparations for a particular military
1904 operation.

1905 2-50. An up-to-date, comprehensive intelligence database is critical to the unit's ability to plan and prepare
1906 rapidly for the range of operations and global environments in which it may operate. GMI supports the
1907 requirement to quickly respond to differing crisis situations with corresponding intelligence spanning the
1908 globe. One of the many places to get information for GMI is the medical intelligence database. The G-2/S-
1909 2 planner develops his initial IPB from GMI products. Additional information on medical intelligence is
1910 found in FM 4-02, FM 4-02.7, FM 4-02.17, FM 4-02.18, and FM 8-42.

1911 2-51. The G-2/S-2 develops and maintains the unit's GMI database on potential threat forces and
1912 environments based on the commander's guidance. As an essential component of intelligence readiness,
1913 this database supports the unit's planning, preparation, execution, and assessment of operations. The G-
1914 2/S-2 applies and updates the database as it executes its intelligence production tasks.

1915 **TARGET INTELLIGENCE**

1916 2-52. Target intelligence is the analysis of enemy units, dispositions, facilities, and systems to identify and
1917 nominate specific assets or vulnerabilities for attack, re-attack, or exploitation (for intelligence). It consists
1918 of two mutually supporting production tasks: target development and combat assessment.

1919 ● Target development is the systematic evaluation and analysis of target systems, system
1920 components, and component elements to determine HVTs for potential attack through
1921 maneuver, fires, or nonlethal means.

1922 ● Once attacked, combat assessment provides a timely and accurate estimate of the affects of the
1923 application of military force (lethal or nonlethal) and information operations on targets and
1924 target systems based on predetermined objectives.

1925 **SCIENTIFIC & TECHNICAL INTELLIGENCE**

1926 2-53. S&TI is the product resulting from the collection, evaluation, analysis, and interpretation of foreign
1927 S&T information. S&TI covers foreign developments in basic and applied research and in applied
1928 engineering techniques and S&T characteristics, capabilities, and limitations of all foreign military
1929 systems, weapons, weapon systems, and materiel, the related research and development (R&D), and the
1930 production methods employed for their manufacture.

1931 2-54. S&TI concerns foreign developments in basic and applied sciences and technologies with warfare
1932 potential. It includes characteristics, capabilities, vulnerabilities, and limitations of all weapon systems,
1933 subsystems, and associated materiel, as well as related R&D. S&TI also addresses overall weapon systems
1934 and equipment effectiveness. Specialized organizations—such as the DIA Missile and Space Intelligence
1935 Center (MSIC), INSCOM, Air Missile Defense, Army Area Air and Missile Defense Command, and
1936 NGIC—produce this category of intelligence. The G-2/S-2 establishes instructions within SOPs, OPORDs,
1937 and OPLANs for handling and evacuating captured enemy materiel (CEM) for S&TI exploitation.

FOR OFFICIAL USE ONLY

1938 **COUNTERINTELLIGENCE**

1939 2-55. As previously defined at the end of chapter 1, CI analyzes the threats posed by foreign intelligence
 1940 and security services and the intelligence activities of non-state actors, such as organized crime, terrorist
 1941 groups, and drug traffickers. CI analysis incorporates all-source information and the results of CI
 1942 investigations and operations to support a multidiscipline analysis of the FP threat.

1943 **ESTIMATIVE**

1944 2-56. Estimates provide forecasts on how a situation may develop and the implications for planning and
 1945 executing military operations. Estimative intelligence goes beyond descriptions of adversary capabilities or
 1946 reporting of enemy activity. It tries to forecast the unknown based on an analysis of known facts using
 1947 techniques such as pattern analysis, inference, and statistical probability.

1948 **UNIFIED ACTION INTELLIGENCE OPERATIONS**

1949 2-57. Joint operations focus and maximize the complementary and reinforcing effects and capabilities of
 1950 each service. JFCs synchronize the complementary capabilities of the Service components that comprise
 1951 the joint force.

1952 2-58. The employment of MI in campaigns and major operations must be viewed from a joint perspective,
 1953 and the intelligence construct must establish a fully interoperable and integrated joint intelligence
 1954 capability. ARFOR intelligence assets work with multinational and interagency partners to accomplish
 1955 their missions. Ideally, multinational and interagency intelligence partners provide cultures, perspectives,
 1956 and capabilities that reinforce and complement Army MI strengths and capabilities. Close intelligence
 1957 coordination is the foundation of successful unified action.

1958 **PERSISTENT SURVEILLANCE AND RELATED ARMY CONSTRUCTS (TACTICAL PERSISTENT
 1959 SURVEILLANCE)**

1960 2-59. A critical part of current operations is the execution of the joint doctrinal concept of persistent
 1961 surveillance. Joint doctrine defines persistent surveillance as:

A collection strategy that emphasizes the ability of some collection systems to linger on demand in an area to detect, locate, characterize, identify, track, target, and possibly provide battle damage assessment and re-targeting in real or near-real time. Persistent surveillance facilitates the formulation and execution of preemptive activities to deter or forestall anticipated adversary courses of action.

1967 2-60. In its simplest form, the goal of the Army construct of joint persistent surveillance is to provide the
 1968 right intelligence to the right person at the right time and in the right format focused to their requirements.
 1969 It is based on the fundamental Army ISR construct and recognizes ISR as a combined arms mission.
 1970 However, these constructs (specifically tactical persistent surveillance) focus on balancing future
 1971 requirements for providing or accessing combat information and intelligence in a networked environment
 1972 to support ongoing operations while also supporting longer-term intelligence analysis and planning and
 1973 other staff functions. Most of the constructs focus on—

- 1974 ● Embedded ISR synchronization capabilities.
- 1975 ● Improved ISR sensor capabilities.
- 1976 ● Assured network communications capability.
- 1977 ● An enterprise approach to analysis, processing, and data and information access across units and
 1978 organizations and echelons.
- 1979 ● Enhanced automated analytical tools to include planning and control and analytical change
 1980 detection capabilities.

FOR OFFICIAL USE ONLY

- 1981 2-61. Within the latest Army intelligence constructs there is recognition that while vast improvements in
1982 ISR capabilities are possible, these new characteristics are not likely to fully develop in the near future. ISR
1983 will—
- 1984 ● Not provide guaranteed and uninterrupted collection on all requirements for all operations.
 - 1985 ● Not change from inherently using a combined arms operational construct.
 - 1986 ● Not eliminate all operational risk and uncertainty.
 - 1987 ● Not obviate the need for operational planning.
 - 1988 ● Not exclusively focus on sensor capability issues.
- 1989 2-62. However, we can expect gradual incremental improvements in—
- 1990 ● Phasing and overlapping of ISR capabilities.
 - 1991 ● Integrating and networking ISR assets and collection efforts.
 - 1992 ● Executing intelligence handover.

1993 **THE NATURE OF LAND OPERATIONS**

1994 2-63. Landpower is the ability—by threat, force, or occupation—to gain, sustain, and exploit control over
1995 land, resources, and people. Army operations reflect expeditionary and campaign capabilities that
1996 constantly adapt to each campaign’s unique circumstances. Expeditionary capabilities require forces
1997 organized to be modular, versatile, and rapidly deployable. Rapidly deployed expeditionary force packages
1998 provide immediate options for seizing or retaining the operational initiative and also allow the conduct of
1999 sustained operations for as long as necessary. Army forces are organized, trained, and equipped for
2000 endurance. The Army’s preeminent challenge is to balance expeditionary agility and responsiveness with
2001 the endurance and adaptability needed to complete a campaign successfully.

2002 2-64. The capability to prevail in close combat is indispensable and unique to land operations. The
2003 outcome of battles and engagements depends on Army forces’ ability to prevail in close combat. Many
2004 factors inherent in land combat combine to complicate the situation. These factors include chaos,
2005 complexity, insufficient intelligence, errors in understanding or planning, difficult terrain, the civilian
2006 population, and an adaptive and lethal enemy. The axiom “intelligence drives operations” continues to be
2007 true especially for land operations. Operations and intelligence are inextricably linked.

- 2008 2-65. Four considerations are preeminent in generating expeditionary capabilities and Army force
2009 packages.
- 2010 ● **Scope.** Considers and strives to understand the threat throughout the depth of an operational
2011 area. Commanders rely on intelligence in order to use maneuver, fires, and other elements of
2012 combat power to defeat or destroy enemy forces.
 - 2013 ● **Duration.** Forces routinely conduct missions prior to, during, and after the commitment of land
2014 combat forces. Intelligence is always engaged.
 - 2015 ● **Terrain.** Missions occur among a complex variety of natural and manmade features. Employing
2016 forces in the complexity of the ground environment requires thorough planning.
 - 2017 ● **Permanence.** Forces are integrated with, or assigned to, land combat forces as they seize or
2018 secure ground.

2019 2-66. Several attributes of the land environment affect the application of landpower. These attributes
2020 include the requirement to deploy and employ Army forces rapidly; the requirement for Army forces to
2021 operate for protracted periods; the nature of close combat; and uncertainty, chance, friction, and
2022 complexity. Reconnaissance, surveillance, and target acquisition (RSTA)/ISR is the means the Army uses
2023 to implement the joint doctrinal concept of persistent surveillance in support of tactical operations.
2024 Dependable technology and responsive intelligence lessen the effects of uncertainty, chance, friction, and
2025 complexity. Complex and dynamic Army tactical operations require extensive ISR capabilities to satisfy
2026 the commander’s information requirements to detect, locate, characterize, identify, track, and target HPTs
2027 and to provide combat assessment in real time within a very fluid operational environment.

FOR OFFICIAL USE ONLY

2028 **2-67. RSTA/ISR is a full spectrum combined arms mission that integrates ground and air**
2029 **capabilities to provide effective, dynamic, timely, accurate, and assured combat information and**
2030 **multidiscipline actionable intelligence for lethal and nonlethal effects and decisions in DS of the**
2031 **ground tactical commander.**

2032 **JOINT INTELLIGENCE OPERATIONS**

2033 2-68. The JTF commanders and their intelligence staffs must—
2034 ● Understand the intelligence requirements of superior, subordinate, and component commands.
2035 ● Identify organic intelligence capabilities and shortfalls.
2036 ● Access combatant command and national systems to ensure appropriate intelligence and CI
2037 products are available to the JTF.

2038 2-69. The JTF's intelligence effort focuses on integrating multi-source information and multi-echelon
2039 intelligence into all-source intelligence products that provide relevant, accurate, and timely knowledge of
2040 the adversary and joint operational area. These products must neither overload the user nor the
2041 communications architecture.

2042 2-70. The J-2 directly supports the JFC's responsibilities for determining objectives, directing operations,
2043 and evaluating the effects of those operations. The J-2 supports the execution of the plan with the
2044 intelligence needed to sustain the operation, attain joint force objectives, provide support to subordinate
2045 commands, and continually support protection. The J-2 analyzes the potential threat situation and provides
2046 assessments to support friendly opportunities. To maintain the initiative, the JFC will seek to get inside the
2047 adversary's decision-making cycle. The J-2 also ensures the provision of the required ISR support to the
2048 JTF and its subordinate functional and service components.

2049 2-71. Figure 2-3 shows a notional JTF J-2 organization. The overall organization of the JTF and operations
2050 will dictate actual composition of the J-2. At a minimum, a core element of analytical, ISR management,
2051 and administrative capabilities is required.

FOR OFFICIAL USE ONLY

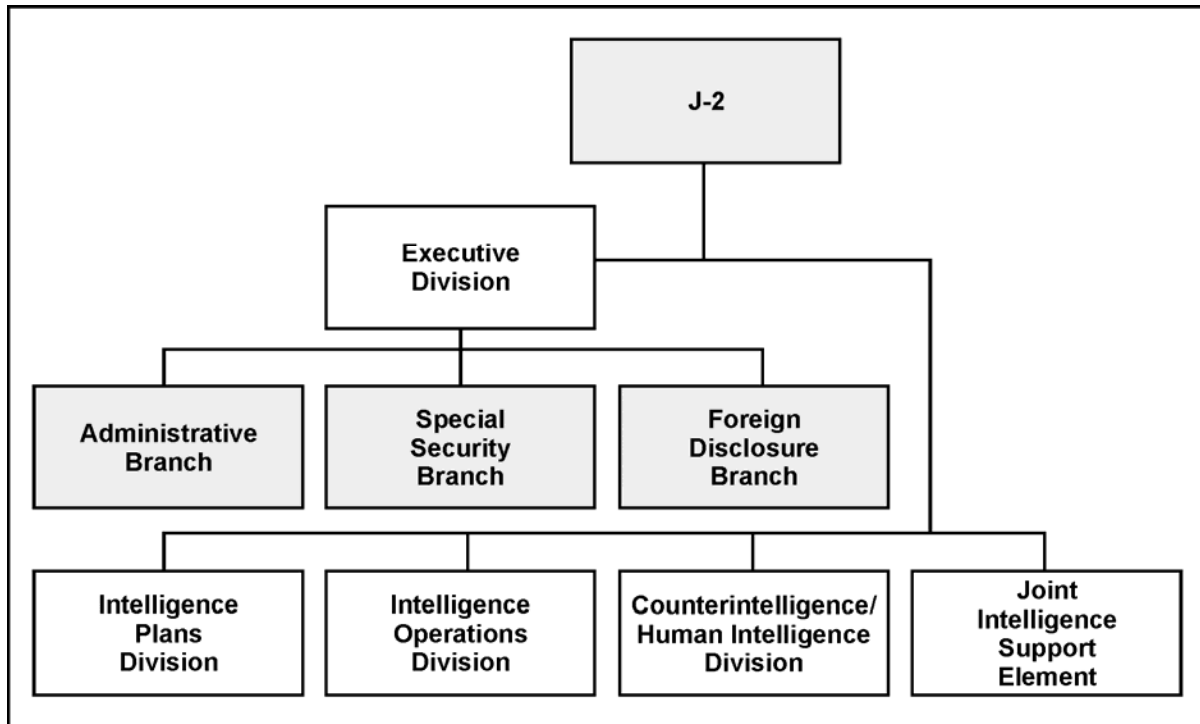


Figure 2-3. Notional joint task force J-2 organization

2052

2053 Considerations in Joint Intelligence Operations

2054 2-72. When conducting joint intelligence operations, there are a number of unique problems that can arise
 2055 due to the complexity of integrating the efforts of the different services and commands. Elements affecting
 2056 joint intelligence operations among the different services include the following:

- 2057 • Intelligence liaison is critical to the success of intelligence operations and requires early
 2058 establishment, particularly between units that have not routinely trained together and possess
 2059 differing capabilities. As a minimum, organizations exchange liaison teams with the higher
 2060 echelon organization. Additional liaison may be necessary to facilitate joint force collection,
 2061 production, or dissemination requirements. Liaison teams—
 - 2062 ■ Support planning and C2 of intelligence operations.
 - 2063 ■ Ensure timely two-way flow of intelligence between commands.
 - 2064 ■ Manage intelligence and resource requirements of the subordinate command.
 - 2065 ■ Advise the commander on service ISR capabilities, limitations, and employment.
- 2066 • Commanders and staffs use IPB to understand the battlefield and develop or refine plans and
 2067 orders. IPB products exchanged between echelons ensure a common picture of the battlefield
 2068 and estimate of the situation.
- 2069 • Communications considerations for joint operations include—
 - 2070 ■ Planning for intelligence communications transition to facilitate execution of branches or
 2071 sequels to the plan or to accommodate shifting of the main effort from one force to another.
 - 2072 ■ Identifying the initial communications architecture to include establishing procedures and
 2073 protocols for information exchanges (databases, text, imagery, voice, and video).

FOR OFFICIAL USE ONLY

- 2074 ■ Balancing the availability of service-unique intelligence systems between echelons or
2075 services. This may require each service providing additional resources. The senior
2076 commander is responsible for allocating resources.
- 2077 ■ Disseminating intelligence between commands and services. Additional communications
2078 equipment, intelligence terminals, and personnel may be required to balance capabilities
2079 between services.
- 2080 ● Identifying the databases each service possesses or has access to; determining which databases
2081 will support the operation and, if necessary, merge them into a single database; and ensure
2082 access by the entire force prior to deployment and/or commencement of operations.
- 2083 ● Providing a focal point for subordinate command access to national or joint intelligence is
2084 essential. The senior commander will request and allocate resources required to support this
2085 access.
- 2086 ● The JFC's intelligence requirements, concept of the operation, and intent drive the ISR effort.
2087 The different organizations and services participating in joint intelligence operations must
2088 continuously share information, intelligence, and products to satisfy requirements. See FM 2-01
2089 for details on intelligence requirements and requirements management. See JP 2-01 for more
2090 information on joint support to military operations.

2091 **Joint Reserve Intelligence Centers**

2092 2-73. A Joint Reserve Intelligence Center (JRIC) is a joint intelligence production and training activity that
2093 uses information networks to link reservist intelligence personnel with the combatant commands, Services,
2094 and/or combat support agencies. A JRIC is located within a Service-owned and managed sensitive
2095 compartmented information (SCI) facility and may also include surrounding collateral and unclassified
2096 areas involved in the performance and direct management of intelligence production work that uses Joint
2097 Reserve Intelligence Program infrastructure and connectivity. The more than 20 JRICs located around the
2098 country are equipped to effectively serve as satellite elements to combatant command JIOCs; however,
2099 they are shared facilities that serve multiple customers and missions (JP 2-0).

2100 **Joint Intelligence Architecture**

2101 2-74. In addition to the J-2 staffs at every joint level of command, the key organizations in the joint
2102 intelligence architecture are the Defense Joint Intelligence Operations Center (DJIOCs), the combatant
2103 command JIOCs, and, when formed, the JTF's joint intelligence support element (JISE). Working together,
2104 these organizations play the primary role in managing and controlling joint intelligence operations. The
2105 formal relationships which link these organizations facilitate information management and optimize
2106 complementary intelligence functions by echelon without obstructing the timely flow of intelligence up,
2107 down, or laterally.

2108 2-75. The DJIOC is the lead DOD intelligence organization responsible for integrating and synchronizing
2109 MI and national intelligence capabilities in support of the combatant commands. The DJIOC collaborates
2110 with the United States Strategic Command's Joint Functional Component Command-Intelligence
2111 Surveillance, and Reconnaissance and Director of National Intelligence (DNI) representatives to formulate
2112 and recommend to the Chairman of the Joint Chiefs of Staff (CJCS), for Secretary of Defense action,
2113 solutions for deconflicting combatant command requirements for national intelligence resources, and
2114 ensures an integrated response to their needs.

2115 2-76. The DJIOC ensures that joint force crisis-related and time-sensitive intelligence requirements are
2116 tasked to the appropriate Service, combatant command, or national agency when the requirements cannot
2117 be satisfied by assigned or attached assets.

FOR OFFICIAL USE ONLY

2118 **Joint Task Force Joint Intelligence Operations Center**

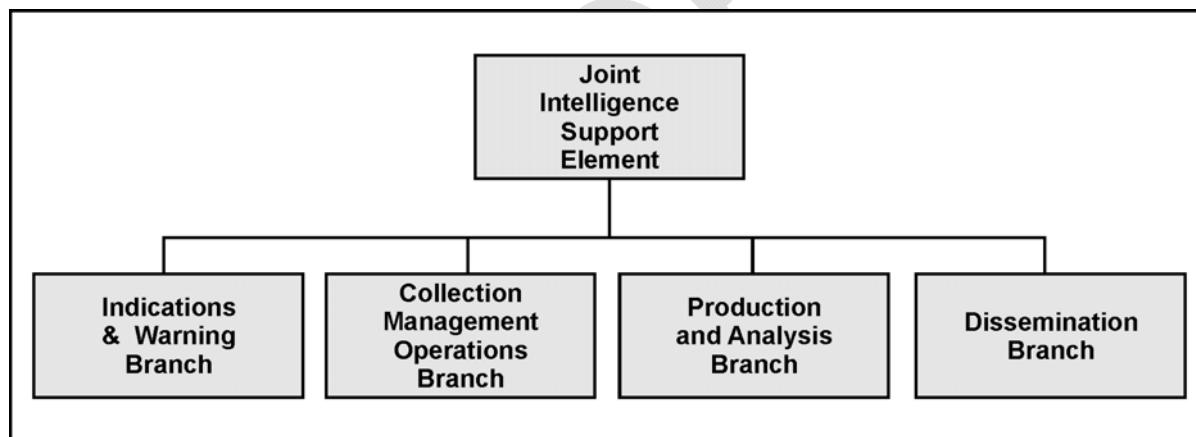
2119 2-77. Combatant command JIOCs are the primary intelligence organizations providing support to joint
 2120 forces at the operational and tactical levels. The JIOC integrates the capabilities of DNI, Service, combat
 2121 support agency, and combatant command intelligence assets to coordinate intelligence planning, collection
 2122 management, analysis, and support.

2123 2-78. The combatant command JIOC is organized in accordance with the CDR's guidance, but normally
 2124 performs the general functions described in JP 2-0 and specific combatant command intelligence TTP.

2125 **Joint Task Force Joint Intelligence Support Element**

2126 2-79. At the discretion of a subordinate JFC, a JTF JISE may be established during the initial phases of an
 2127 operation to augment the subordinate joint force J-2 element. Under the direction of the J-2, the JISE
 2128 normally manages the intelligence collection, production, and dissemination for the JTF. The JISE
 2129 provides intelligence to JTF operational forces and performs common intelligence functions.

2130 2-80. By design, the JISE is scalable and can expand to meet the needs of the JTF and the operating
 2131 environment. It is composed of analytical experts, analysis teams, and ISR managers that provide services
 2132 and products, which the JTF, JTF staff, and subordinate components require. These experts focus on
 2133 solving the JTF commander's operational intelligence problems. The JISE's capability to perform all-
 2134 source analysis and ISR synchronization is key to producing operational intelligence that is timely,
 2135 relevant, accurate, predictive, and targeted. Figure 2-4 illustrates the features of a typical JISE.



2136 **Figure 2-4. Typical joint intelligence support element**

2137 **Joint Task Force Intelligence Organizations**

2138 2-81. In addition to the JISE, the JTF commander and J-2 may require other supporting JIOCs or teams
 2139 based on projected operations. The JTF commander may make a request to the DJIOC for specific national
 2140 intelligence agency capabilities. The DJIOC evaluates and coordinates the JTF commander's requirements
 2141 with the J-3, J-5, and national intelligence agencies and tailors the composition of the deployment packages
 2142 to meet those needs.

2143 2-82. The deployment packages, such as the National Intelligence Support Team (NIST), provide access to
 2144 the entire range of capabilities resident in the national intelligence agencies and can focus those capabilities
 2145 on the JTF commander's intelligence requirements. The J-2X manages and coordinates the HUMINT and
 2146 CI activities of national, combatant command, and service components operating within the JTF's joint
 2147 operational area. The Joint Captured Materiel Exploitation Center (JCMEC) assists in management of
 2148 recovery, exploitation, and disposal of captured enemy equipment (CEE). The JTF commander's

FOR OFFICIAL USE ONLY

2149 requirements dictate the composition and tailoring of such deployment packages. See JP 3-33 for more
2150 information on JTF intelligence organizations.

2151 **Augmentation Considerations**

2152 2-83. Depending on the scale of the operations, the intelligence organizations described above and those of
2153 the JTF's subordinate command may require personnel augmentation. Optimum use of available
2154 intelligence assets is essential to ensure quality support in meeting the JTF commander's requirements. The
2155 JTF J-2 should identify intelligence personnel augmentation requirements in accordance with the CJCS
2156 Instruction 1301.01. The CCDR and the JTF refine personnel requirements and initiate requests when they
2157 anticipate or start an operation.

2158 2-84. A consideration for the JTF when requesting support or augmentation is that these national level
2159 teams and individual augmentees are not totally self-contained elements; rather they require logistic,
2160 information, and other support from the supported command. Each deployment is unique based on mission,
2161 duration, team composition, and capabilities required. A full NIST, for example, requires a private, access-
2162 controlled area within a sensitive compartmented SCI facility work environment and dedicated secure
2163 communications.

2164 2-85. For more information on intelligence operations as they apply to other armed services, see the
2165 individual service intelligence doctrine. See also JP 2-0 series, JP 3-0, and JP 5-0 for details on joint
2166 intelligence operations and considerations.

2167 **Multinational Intelligence**

2168 2-86. Multinational intelligence operations take place within the structure of an alliance or coalition. Some
2169 multinational military organizations, such as the North Atlantic Treaty Organization and the UN Command
2170 in the Republic of Korea, are highly structured and enduring. Others, such as the coalition formed during
2171 the Gulf War, are less formal and temporary.

2172 2-87. In multinational operations, the multinational force commander exercises command authority over a
2173 military force composed of elements from two or more nations. Therefore, in most multinational
2174 operations, the JTF must share intelligence, as necessary, for mission accomplishment with foreign military
2175 forces and coordinate exchange of intelligence with those forces.

2176 2-88. In some circumstances, the JTF may need to seek authority to go outside the usual political-military
2177 channels to provide information to NGOs. The JTF must tailor intelligence policy and dissemination
2178 criteria to each multinational operation.

2179 2-89. The minimum requirements for sharing intelligence, how intelligence is cleared for sharing, and the
2180 specific means for intelligence sharing will be situationally dependent. See FM 3-16 and the ABCA
2181 Coalition Operations Handbook for more information about intelligence considerations in multinational
2182 operations.

2183 **FORCE PROJECTION OPERATIONS**

2184 2-90. Force projection is the military component of power projection. It is a central element of the national
2185 military strategy. Army organizations and installations linked with joint forces and industry form a
2186 strategic platform to maintain, project, and sustain ARFOR wherever they deploy. Force projection
2187 operations are inherently joint and require detailed planning and synchronization. As discussed below,
2188 force projection encompasses a range of processes—mobilization, deployment, employment, sustainment,
2189 and redeployment.

2190 2-91. The Army must change its mindset from depending on an "intelligence buildup" to performing
2191 intelligence readiness on a daily basis in order to meet the requirements for strategic responsiveness. MI
2192 personnel, even in garrison at the lowest tactical echelons, must use their analytic and other systems and

FOR OFFICIAL USE ONLY

2193 prepare for possible operations on a daily basis. When a unit has an indication that it may be deployed or
2194 have a contingency mission in an area of the world, they can begin to generate intelligence knowledge on
2195 their projected AO.

2196 2-92. Built on a foundation of intelligence readiness, the intelligence warfighting function provides the
2197 commander with the intelligence needed to plan, prepare, and execute force projection operations.
2198 Successful intelligence during force projection operations relies on continuous collection and intelligence
2199 production before and during the operation. In a force projection operation, higher echelons will provide
2200 intelligence to lower echelons until the tactical ground force completes entry and secures the lodgment
2201 area. The joint force J-2 must exercise judgment when providing information to subordinate G-2s/S-2s to
2202 avoid overwhelming them.

2203 2-93. Key planning factors for intelligence in force projection include—

- 2204 ● Stay out front in intelligence planning:
 - 2205 ■ Begin to generate intelligence knowledge as soon as possible.
 - 2206 ■ Develop a steady effort.
 - 2207 ■ Prioritize intelligence requirements for surge.
- 2208 ● Understand how to get intelligence support:
 - 2209 ■ Identify information and asset requirements.
 - 2210 ■ Know what is available and how and when to get it.

2211 2-94. The G-2/S-2 must anticipate, identify, consider, and evaluate all threats to the entire unit throughout
2212 force projection operations. This is critical during the deployment and entry operations stages of force
2213 projection. During these stages, the unit is particularly vulnerable to enemy actions because of its limited
2214 combat power and knowledge of the AO. Intelligence personnel must, therefore, emphasize the delivery of
2215 combat information and intelligence products that indicate changes to the threat or AO developed during
2216 predeployment IPB. The G-2/S-2 should—

- 2217 ● Review available databases on assigned contingency AOIs, conduct IPB on these AOIs, and
2218 develop appropriate IPB products.
- 2219 ● Comply with higher headquarters SOPs and manuals for specific intelligence operations
2220 guidance.
- 2221 ● Coordinate for and rehearse electronic message transfers (for example, Internet Protocol
2222 addresses, routing indicators) using the same communications protocols with theater, higher
2223 headquarters, subordinate, and lateral units that the unit would use when deployed.
- 2224 ● Plan, train, and practice surging intelligence functions on likely or developing contingency
2225 crises.
- 2226 ● Prepare and practice coordination from predeployment through redeployment with other
2227 elements and organizations (for example, HUMINT, IMINT, SIGINT, MASINT, information
2228 operations, staff weather officer, CA, PSYOP, and SOF units, to include databases and
2229 connectivity).
- 2230 ● Include the following as a part of daily (sustainment) operations:
 - 2231 ■ USAR and other augmentation.
 - 2232 ■ A linguist plan with proficiency requirements. (Alert linguists through early entry phases of
2233 deployment.)
 - 2234 ■ Training (individual and collective).
- 2235 ● Establish formal or informal intelligence links, relationships, and networks to meet developing
2236 contingencies.
- 2237 ● Forward all RFIs to higher headquarters in accordance with SOPs.
- 2238 ● Establish statements of intelligence interests, other production, and I&W requirements.

FOR OFFICIAL USE ONLY

- 2239 2-95. To draw intelligence from higher echelons and focus intelligence downward, based on the
 2240 commander's needs, the G-2/S-2 must—
- 2241 ● Understand the J-2's multiple echelon and broadcast dissemination capability to ensure near-real
 2242 time (NRT) reporting to all deployed, in transit, or preparing to deploy forces.
 - 2243 ● Maintain or build intelligence databases on the environment and threats for each probable
 2244 contingency.
 - 2245 ● State and record the CCIR (as a minimum, list the PIRs and ISR tasks or requests).
- 2246 2-96. Until the unit's collection assets become operational in the AO, the G-2/S-2 will depend upon
 2247 intelligence from the ARFOR or JTF to answer the unit's intelligence needs. Intelligence and ISR
 2248 considerations during force projection are discussed below.

2249 **MOBILIZATION**

- 2250 2-97. Mobilization is the process by which the armed forces or part of them are brought to a state of
 2251 readiness for war or other national emergency. It assembles and organizes resources to support national
 2252 objectives. Mobilization includes activating all or part of the USAR, and assembling and organizing
 2253 personnel, supplies, and materiel. A unit may be brought to a state of readiness for a specific mission or
 2254 other national emergency. This process, called mobilization, is where specific US Active Army, ARNG,
 2255 ARNGUS, and USAR units, capabilities, and personnel are identified and integrated into the unit. During
 2256 mobilization, the G-2/S-2 must—
- 2257 ● Monitor intelligence reporting on threat activity and I&W data.
 - 2258 ● Manage IRs and RFIs from their unit and subordinate units to include updating ISR planning.
 - 2259 ● Establish habitual training relationships with their US Active Army, ARNG, ARNGUS, and
 2260 USAR augmentation units and personnel as well as higher echelon intelligence organizations as
 2261 identified in the existing OPLAN.
 - 2262 ● Support the USAR units and augmentation personnel by preparing and conducting intelligence
 2263 training and threat update briefings and by disseminating intelligence.
 - 2264 ● Identify ISR force requirements for the different types of operations and contingency plans.
 - 2265 ● Identify individual military, civilian, and contractor augmentation requirements for intelligence
 2266 operations. The Army, and the Intelligence warfighting function in particular, cannot perform its
 2267 missions without the support of its Department of the Army Civilians and contractors. The force
 2268 increasingly relies on the experience, expertise, and performance of non-uniformed personnel
 2269 and has fully integrated these non-uniformed personnel into the warfighting team.
- 2270 2-98. During mobilization the G-2/S-2, in conjunction with the rest of the staff, must ensure the adequacy
 2271 of training and equipping of US Army Active and USAR MI organizations and individual augmentees to
 2272 conduct intelligence operations. Predictive intelligence also supports the decisions the commander and staff
 2273 must make about the size, composition, structure, and deployment sequence of the force in order to create
 2274 the conditions for success.
- 2275 2-99. The G-2/S-2 supports peacetime contingency planning with IPB products and databases on likely
 2276 contingency areas. The G-2/S-2 establishes an intelligence synchronization plan that will activate upon
 2277 alert notification. For smooth transition from predeployment to entry, the G-2/S-2 must coordinate
 2278 intelligence synchronization and communications plans before the crisis occurs. The intelligence
 2279 synchronization plan identifies the intelligence requirements supporting those plans, to include—
- 2280 ● ISR assets providing support throughout the AOI.
 - 2281 ● Command and support relationships of ISR assets at each echelon.
 - 2282 ● Report and request procedures not covered in unit SOPs.
 - 2283 ● Sequence of deployment of ISR personnel and equipment. Early deployment of key ISR
 2284 personnel and equipment is essential for FP and combat readiness. Composition of initial and

FOR OFFICIAL USE ONLY

- 2285 follow-on deploying assets is influenced by the factors of METT-TC, availability of
2286 communications, and availability of lift.
- 2287 ● Communications architecture supporting both intelligence staffs and ISR assets.
 - 2288 ● Friendly vulnerabilities to hostile intelligence threats and plans for conducting FP measures. The
 - 2289 staff must begin this type of planning as early as possible to ensure adequate support to FP of
 - 2290 deploying and initial entry forces.
 - 2291 ● Monitor time-phased force and deployment data (TPFDD) and recommend changes in priority
 - 2292 of movement, unit, or capability to enable ISR operations.

2293 2-100. The G-2/S-2 must continually monitor and update the OPLANs to reflect the evolving situation,
2294 especially during crisis situations. National intelligence activities monitor regional threats throughout the
2295 world and can answer some intelligence requirements supporting the development of OPLANs.

2296 2-101. Upon alert notification, the G-2/S-2 updates estimates, databases, IPB products, and other
2297 intelligence products needed to support command decisions on force composition, deployment priorities
2298 and sequence, and the AOI. Units reassess their collection requirements immediately after alert
2299 notification. The G-2/S-2 begins verifying planning assumptions within the OPLANs. CI and ISR
2300 personnel provide FP support and antiterrorism measures.

2301 2-102. Throughout mobilization, unit intelligence activities will provide the deploying forces with the
2302 most recent intelligence on the AO. The intelligence staff will also update databases and situation graphics.
2303 The G-2/S-2 must—

- 2304 ● Fully understand the unit, ARFOR, and joint force intelligence organizations.
- 2305 ● Revise intelligence and intelligence-related communications architecture and delete or integrate
- 2306 any new systems and software with the current architecture.
- 2307 ● Support 24-hour operations and provide continuous intelligence.
- 2308 ● Plan all required intelligence reach procedures.
- 2309 ● Determine transportation availability for deployment and availability when deployed.
- 2310 ● Determine all sustainability requirements.
- 2311 ● Determine intelligence release requirements and restrictions; releasability to multinational and
- 2312 HN sources.
- 2313 ● Review status of forces agreements (SOFAs), ROE, international laws, and other agreements,
- 2314 emphasizing the effect that they have on intelligence collection operations. (Coordinate with the
- 2315 staff judge advocate on these issues.)
- 2316 ● Ensure ISR force deployment priorities are reflected in the TPFDD to support ISR operations
- 2317 based upon the factors of METT-TC.
- 2318 ● Ensure intelligence links provide the early entry commander vital access to multi-source army
- 2319 and joint intelligence collection assets, processing systems, and databases.
- 2320 ● Review the supporting unit commanders' specified tasks, implied tasks, task organization,
- 2321 scheme of support, and coordination requirements with forward maneuver units. Address issues
- 2322 or shortfalls and direct or coordinate changes.
- 2323 ● Establish access to national HUMINT, **Error! Bookmark not defined.**IMINT, SIGINT,
- 2324 MASINT, and CI databases, as well as automated links to joint service, multinational, and HN
- 2325 sources.

2326 **DEPLOYMENT**

2327 2-103. Deployment is the movement of forces and materiel from their point of origin to the AO. This
2328 process has four supporting components: predeployment activities, fort-to-port, port-to-port, and port-to-
2329 destination. Success in force projection operations hinges on timely deployment. The size and composition
2330 of forces requiring lift are based on the factors of METT-TC, availability of pre-positioned assets, the

FOR OFFICIAL USE ONLY

2331 capabilities of HN support, and the forward presence of US forces. Force tailoring is the process used to
 2332 determine the correct mix and sequence of deploying units.

2333 2-104. During deployment, intelligence organizations at home station or in the rear area take advantage of
 2334 modern satellite communications, broadcast technology, and automated data processing systems to provide
 2335 graphic and textual intelligence updates to the forces enroute. Enroute updates help eliminate information
 2336 voids and, if appropriate, allow the commander to adjust the plan prior to arrival in JOA in response to
 2337 changes in the operational environment.

2338 2-105. Intelligence units extend established networks to connect intelligence staffs and collection assets at
 2339 various stages of the deployment flow. Where necessary, units establish new communications paths to
 2340 meet unique demands of the mission. If deployed, theater and corps analysis and control elements play a
 2341 critical role in making communications paths, networks, and intelligence databases available to deploying
 2342 forces.

2343 2-106. Space-based systems are key to supporting intelligence during the deployment and the subsequent
 2344 stages of force projection operations by—

- 2345 ● Monitoring terrestrial AOIs through ISR assets to help reveal enemy location and disposition,
 2346 attempting to identify the enemy's intent.
- 2347 ● Providing communications links between forces enroute and in the continental United States
 2348 (CONUS).
- 2349 ● Permitting MI collection assets to accurately determine their position through the Global
 2350 Positioning System.
- 2351 ● Providing timely and accurate data on meteorological, oceanographic, and space environmental
 2352 factors that might affect operations.
- 2353 ● Providing warning of theater ballistic missile launches.
- 2354 ● Providing timely and accurate weather information to all commanders through the Integrated
 2355 Meteorological System.

2356 2-107. Situation development dominates intelligence operations activities during initial entry operations.
 2357 The G-2/S-2 attempts to identify all threats to arriving forces and assists the commander in developing FP
 2358 measures. During entry operations, echelons above corps organizations provide intelligence. This support
 2359 includes providing access to departmental and joint intelligence and deploying scalable intelligence assets.
 2360 The entire effort focuses downwardly to provide tailored support to deploying and deployed echelons in
 2361 response to their CCIRs (PIRs and FFIR).

2362 2-108. Collection and processing capabilities are enhanced, as collection assets build up in the
 2363 deployment area, with emphasis on the build-up of the in-theater capability required to conduct sustained
 2364 ISR operations. As the build-up continues, the G-2/S-2 strives to reduce total dependence on extended
 2365 split-based intelligence from outside the AO. As assigned collection assets arrive into the JOA, the G-2/S-2
 2366 begins to rely on them for tactical intelligence although higher organizations remain a source of
 2367 intelligence.

2368 2-109. As the ARFOR headquarters arrives in the JOA, the joint force J-2 implements and, where
 2369 necessary, modifies the theater intelligence architecture. Deploying intelligence assets establishes liaison
 2370 with staffs and units already present in the AO. Liaison personnel and basic communications should be in
 2371 place prior to the scheduled arrival of parent commands. ISR units establish intelligence communications
 2372 networks.

2373 2-110. CONUS and other relatively secure intelligence bases outside the AO continue to support
 2374 deployed units. Systems capable of rapid receipt and processing of intelligence from national systems and
 2375 high capacity, long-haul communications systems are critical to the success of split-based support of a
 2376 force projection operation. These systems provide a continuous flow of intelligence to satisfy many
 2377 operational needs.

FOR OFFICIAL USE ONLY

2378 2-111. The G-2/S-2, in coordination with the G-3/S-3, participates in planning to create conditions for
2379 decisive operations. The G-2/S-2 also adjusts collection activities as combat power strength builds. During
2380 entry operations the G-2/S-2—

- 2381 ● Monitors FP indicators.
- 2382 ● Monitors the ISR capability required to conduct sustained intelligence operations.
- 2383 ● Monitors intelligence reporting on threat activity and I&W data.
- 2384 ● Develops measurable criteria to evaluate the results of the intelligence synchronization plan.
- 2385 ● Assesses—
 - 2386 ■ Push versus pull requirements of intelligence reach.
 - 2387 ■ Effectiveness of the intelligence communications architecture.
 - 2388 ■ Reporting procedures and timelines.
 - 2389 ■ Intelligence to OPLANs and OPORDs, branches, and sequels (to include planning follow-
2390 on forces).

2391 **ENTRY OPERATIONS**

2392 2-112. Enemies often possess the motives and means to interrupt the deployment flow of Army forces.
2393 Threats to deploying forces may include advanced conventional weaponry (air defense, mines) and
2394 weapons of mass destruction. Sea and air ports of debarkation should be regarded as enemy HPTs because
2395 they are the entry points for forces and equipment. Ports of debarkation are vulnerable because they are
2396 fixed targets with significant machinery and equipment that is vulnerable to attack; in addition to military
2397 forces and materiel, HN support personnel, contractors, and civilians may all be working there.

2398 2-113. An enemy attack, or even the threat of an enemy attack, on a port of debarkation can have a major
2399 impact on force projection momentum. Commanders at all levels require predictive intelligence so that they
2400 may focus attention on security actions that reduce vulnerabilities. To avoid, neutralize, or counter threats
2401 to entry operations, the commanders rely on the ability of the G-2/S-2 to support future operations by
2402 accurately identifying enemy reactions to US actions, anticipating their response to our counteractions and
2403 predicting additional enemy COAs.

2404 **SUSTAINMENT**

2405 2-114. Sustainment involves providing and maintaining levels of personnel and materiel required to
2406 sustain the operation throughout its duration. Sustainment may be split-based between locations within and
2407 outside continental United States (OCONUS). For intelligence, sustainment may be focused on force
2408 rotation—ensuring that intelligence personnel or units entering an established AO have current intelligence
2409 and the appropriate level of detailed knowledge of ongoing intelligence operations. This includes providing
2410 data file updates through the generate intelligence knowledge step of the intelligence process prior to the
2411 deployment of replacement personnel or units as well as a coordinated intelligence hand-off of ongoing
2412 intelligence operations such as military source operations. Sustainment also includes ensuring units have
2413 the MI assets required to accomplish the mission, such as personnel (including linguists), communications
2414 systems, ISR systems, and appropriate maintenance support.

2415 **REDEPLOYMENT**

2416 2-115. Redeployment is the process by which units and materiel reposture themselves in the same theater;
2417 transfer forces and materiel to support another JFC's operational requirements; or return personnel and
2418 materiel to the home or demobilization station upon completion of the mission. Redeployment operations
2419 encompass four phases:

- 2420 ● Recovery, reconstitution, and predeployment activities.
- 2421 ● Movement to and activities at the port of embarkation.
- 2422 ● Movement to the port of debarkation.

FOR OFFICIAL USE ONLY

- 2423 • Movement to homestation.
- 2424 2-116. As combat power and resources decrease in the AO, FP and I&W become the focus of the
2425 commander's intelligence requirements. This in turn drives the selection of those assets that must remain
2426 deployed until the end of the operation and those that may redeploy earlier. The S-2—
- 2427 • Monitors intelligence reporting on threat activity and I&W data.
2428 • Continues to conduct intelligence to FP.
2429 • Requests ISR support (theater and national systems) and intelligence in support of
2430 redeployment.
- 2431 2-117. After redeployment, MI personnel and units recover and return to predeployment activities. ISR
2432 units resume contingency-oriented peacetime intelligence operations. USAR ISR units demobilize and
2433 return to peacetime activities. G-2/S-2s must—
- 2434 • Monitor intelligence reporting on threat activity and I&W data.
2435 • Update or consolidate databases.
2436 • Maintain intelligence readiness.
2437 • Provide their input into the Force Design Update process to refine modified table of
2438 organizations and equipment and evaluate the need for individual mobilization augmentee
2439 personnel.
2440
2441

FOR OFFICIAL USE ONLY

2442

PART TWO

2443

Intelligence in Full Spectrum Operations

2444

Part Two discusses the role of intelligence and the intelligence warfighting function within full spectrum operations and the interaction of the intelligence process with the operations process. It describes how both MI and the intelligence warfighting function provide commanders and warfighters with the intelligence they require in order to drive operations.

2445

2446

2447

2448

2449

Chapter 3 discusses the role of intelligence within full spectrum operations. It provides an overview of intelligence readiness, particularly the intelligence requirements associated with force projection. The doctrinal concept of MI asset technical channels is discussed as a complement to, not a replacement of, the Army's command and support relationships.

2450

2451

2452

2453

2454

Chapter 4 presents the intelligence process, describes its interaction with the operations process, and discusses the methodology that accomplishes the primary focus of intelligence in full spectrum operations, to provide the warfighter with effective intelligence.

2455

2456

2457

2458

Chapter 3

2459

Fundamentals in Full Spectrum Operations

2460

THE OPERATIONAL CONCEPT

2461

3-1. *The Army's operational concept is full spectrum operations: Army forces combine offensive, defensive, and stability or civil support operations simultaneously as part of an interdependent joint force to seize, retain, and exploit the initiative, accepting prudent risk to create opportunities to achieve decisive results. They employ synchronized action—lethal and nonlethal—proportional to the mission and informed by a thorough understanding of all variables of the operational environment. Mission command that conveys intent and appreciation of all aspects of the situation guides the adaptive use of Army forces (FM 3-0).*

2462

2463

2464

2465

2466

2467

2468

3-2. Intelligence supports the commander across full spectrum operations. It helps the commander decide when and where to concentrate sufficient defeat threat COAs. ISR is essential for the commander to achieve surprise against the threat, preclude surprise from the threat, maintain the initiative on the battlefield, and win battles. Commanders and staffs at all levels synchronize intelligence with the other warfighting functions to maximize their ability to see and strike the enemy simultaneously throughout the AO.

2469

2470

2471

2472

2473

2474

3-3. Every Soldier in the command is responsible for detecting and reporting threat activities, dispositions, and capabilities. In order to accomplish this, the task of Soldier surveillance and reconnaissance was developed to help commanders get combat information and reports. This task is critical because the environment we operate in is characterized by violence, uncertainty, complexity, and asymmetric methods by the threat. The Every Soldier is a Sensor program is supported through Soldier

2475

2476

2477

2478

FOR OFFICIAL USE ONLY

2479 surveillance and reconnaissance. (See FM 2-91.6 for a detailed discussion of Soldier surveillance and
2480 reconnaissance.)

2481 3-4. The increased situational awareness that Soldiers develop through personal contact and observation
2482 is a critical element of that unit's ability to more fully understand the battlefield. Soldiers collect combat
2483 information that is then processed into intelligence by unit intelligence analysts. While medical personnel
2484 cannot be assigned ISR tasks due to their Geneva Convention category status, medical personnel who gain
2485 information through casual observation of activities in plain view while discharging their humanitarian
2486 duties will report the information to their supporting intelligence element.

2487 **INTELLIGENCE SUPPORT TO THE ELEMENTS OF FULL**
2488 **SPECTRUM OPERATIONS**

2489 3-5. Full spectrum operations require continuous, simultaneous combinations of offensive, defensive, and
2490 stability or civil support tasks. Intelligence through ISR facilitates understanding of the portions of the
2491 mission variables of enemy, terrain, weather, and civil considerations, the latter in coordination with the
2492 G-9/S-9. This allows the commander to conduct operations at a time and place of our choosing rather than
2493 reacting to enemy operations. Operations are organized as decisive, shaping, and sustaining.

2494 **OFFENSIVE OPERATIONS**

2495 3-6. *Offensive operations are combat operations conducted to defeat and destroy enemy forces and seize*
2496 *terrain, resources, and population centers* (FM 3-0). Offensive operations at all levels require effective
2497 intelligence to help the commander avoid the enemy's main strength and to deceive and surprise the
2498 enemy. During offensive operations, intelligence must provide the commander with updated IPB products
2499 and an intelligence running estimate in a timely manner for the commander to significantly affect the
2500 enemy. The intelligence running estimate ensures commanders have the intelligence they need to conduct
2501 offensive operations with minimum risk of surprise.

2502 3-7. The G-2/S-3 develops IPB products to assist the commander in identifying all aspect within the AO
2503 or AOI that will affect mission accomplishment. The entire staff, led by the echelon intelligence staff, uses
2504 the IPB process to identify any aspects of the AO or AOI that will affect enemy, friendly, and third-party
2505 operations. The IPB process is collaborative in nature and requires information from all staff elements and
2506 some subordinate units. All staff and subordinate elements use the results and products of the IPB process
2507 for planning. FM 2-01.3 describes the IPB process.

2508 3-8. The G-2/S-2 supports the commander's use of unit ISR assets to analyze the terrain and confirm or
2509 deny the enemy's strengths, dispositions, and likely intentions. These assets also gather information
2510 concerning the civilian considerations within the AO. The G-2/S-2 and operations officers, in coordination
2511 with the rest of the staff, develop an integrated ISR plan that satisfies the commander's maneuver,
2512 targeting, and information requirements.

- 2513 3-9. In offensive operations, a commander's information requirements often include—
- 2514 ● Locations, composition, equipment, strengths, and weaknesses of the defending enemy force, to
2515 include high-payoff targets (HPTs) and enemy ISR capabilities.
 - 2516 ● Locations of possible enemy assembly areas.
 - 2517 ● Locations of enemy indirect fire weapon systems and units.
 - 2518 ● Locations of gaps and assailable flanks.
 - 2519 ● Locations of areas for friendly and enemy air assaults.
 - 2520 ● Locations of enemy air defense gun and missile units.
 - 2521 ● Locations of enemy electronic warfare (EW) units.
 - 2522 ● Effects of terrain and weather and civil considerations on current and projected operations.
 - 2523 ● Numbers, routes, and direction of movement of dislocated civilians.

FOR OFFICIAL USE ONLY

- 2524 ● Withdrawal routes for enemy forces.
- 2525 ● Anticipated timetable schedules for the enemy’s most likely COA and other probable COAs.
- 2526 ● Locations of enemy C2 and ISR systems and the frequencies used by the information systems
- 2527 linking these systems.

2528 **DEFENSIVE OPERATIONS**

2529 3-10. Defensive operations are combat operations conducted to defeat an enemy attack, gain time,
 2530 economize forces, and develop conditions favorable for offensive or stability operations. The immediate
 2531 purpose of defensive operations is to defeat an enemy attack. Commanders defend to buy time, hold key
 2532 terrain, hold the enemy in one place while attacking in another, or destroy enemy combat power while
 2533 reinforcing friendly forces.

2534 3-11. Intelligence should determine the enemy's strength, COAs, and location of enemy follow-on forces.
 2535 Defending commanders can then decide where to arrange their forces in an economy-of-force role to
 2536 defend and shape the battlefield. Intelligence support affords commanders the time necessary to commit the
 2537 striking force precisely.

2538 3-12. Intelligence supports the commander’s defensive operations with IPB products to identify probable
 2539 enemy objectives and various approaches; patterns of enemy operations; the enemy’s vulnerability to
 2540 counterattack, interdiction, EW, air attacks, and canalization by obstacles; and the enemy’s capability to
 2541 conduct air attacks against his force, insert forces behind friendly units, and employ CBRNE weapons. The
 2542 G-2/S-2 must also evaluate how soon follow-on forces can join the fight against an enemy attacking in
 2543 echelons.

2544 3-13. The G-2/S-2 also supports the commander with synchronization of ISR operations to answer the
 2545 CCIRs. ISR operations must be continuously assessed and updated during operations. The ISR plan must
 2546 provide early identification of as many of the commander’s requirements as possible. It is critical that the
 2547 G-2/S-2 support the commander’s ability to see the enemy during the conduct of all defensive operations.
 2548 In defensive operations, these requirements often include—

- 2549 ● Locations, composition, equipment, strengths, and weaknesses of the advancing enemy force.
- 2550 ● Enemy reconnaissance objectives or goals.
- 2551 ● Locations of possible enemy assembly areas.
- 2552 ● Locations of enemy indirect fire weapon systems and units.
- 2553 ● Locations of gaps, assailable flanks, and other enemy weaknesses.
- 2554 ● Locations of areas for enemy helicopter and parachute assaults.
- 2555 ● Locations of artillery and air defense gun and missile units.
- 2556 ● Locations of enemy EW of civilian populations.
- 2557 ● Effects of terrain and weather and civil considerations on current and projected operations.
- 2558 ● Likely withdrawal routes for enemy forces.
- 2559 ● Numbers, routes, and direction of movement of dislocated civilians.
- 2560 ● Anticipated timetable for the enemy’s most likely COA.
- 2561 ● Locations of enemy command posts, fire direction control centers, EW sites, and target
- 2562 acquisition sensor and target fusion sites and the frequencies they are using.

2563 **STABILITY OPERATIONS**

2564 3-14. *Stability operations encompass various military missions, tasks, and activities conducted outside the*
 2565 *US in coordination with other instruments of national power to maintain or reestablish a safe and secure*
 2566 *environment, provide essential governmental services, emergency infrastructure reconstruction, and*
 2567 *humanitarian relief (JP 3-0).*

FOR OFFICIAL USE ONLY

2568 3-15. The environment is often much more complex during stability operations and as a result intelligence
2569 is often more complex. Elements of combat power are discussed below. As a result, commanders must be
2570 even more involved in and knowledgeable of ISR during stability operations.

2571 3-16. In stability operations, commanders often require even more detailed intelligence and IPB products
2572 necessary to determine how best to influence the environment and enhance regional stability. The
2573 identification and analysis of the threat, terrain, weather, and civil considerations (civil considerations are
2574 described using the acronym ASCOPE) are important in conducting stability operations. A lack of
2575 knowledge concerning insurgents, how to separate local combatants, local politics, customs, and culture
2576 could lead to US actions which attack unsuitable targets or which may offend or cause mistrust among the
2577 local population. This could potentially threaten mission accomplishment.

2578 **CIVIL SUPPORT OPERATIONS**

2579 3-17. *Civil support is the Department of Defense support to U.S. civil authorities for domestic*
2580 *emergencies, and for designated law enforcement and other activities (JP 1-02).* Civil support includes
2581 operations that address the consequences of natural or manmade disasters, accidents, terrorist attacks, and
2582 incidents within the United States and its territories. Army forces conduct civil support operations when the
2583 size and scope of events exceed the capabilities or capacities of domestic civilian agencies.

2584 3-18. The ARNG often acts as a first military responder for civil support operations on behalf of State
2585 authorities while serving in State active duty status or when functioning under Title 32 U.S. Code
2586 authority. State active duty status refers to ARNG forces and State defense force personnel under State
2587 control. In State active duty status, the State Governor commands the ARNG and the State defense force.
2588 The State defense force is sometimes known as the State organized defense force or State militia (some
2589 States do not have a State defense force). Missions are planned and executed in accordance with the needs
2590 of the State and within the guidelines of State laws and statutes. ARNG forces in State active duty status
2591 can perform civil law enforcement missions in accordance with the laws and statutes of their State.

2592 3-19. Intelligence support in civil support operations is conducted strictly within the guidelines of US law
2593 and focused on the specific missions directed by the Secretary of Defense. IPB can identify natural threats
2594 and hazards such as areas likely to flood during heavy rain or in the event of a dam or levee break.

2595 3-20. Intelligence analysts can fuse the information from a variety of DOD supporting agencies and
2596 develop information and intelligence products to answer PIRs. Intelligence analysis can also assist local
2597 authorities in identifying areas in which the military can provide support in restoring essential services. ISR
2598 assets can assist search and rescue, damage assessment, potential hazards, and locating displaced persons.
2599 ISR assets can also help identify CBRNE materiel and weapons manufacturing and storage locations. ISR
2600 assets require authorization from the Secretary of Defense. For more information on intelligence support to
2601 civil support operations, see FMI 2-91.501.

2602 **ELEMENTS OF COMBAT POWER**

2603 3-21. *Combat power is the total means of destructive, constructive, and information capabilities which a*
2604 *military unit or formation can apply at a given time. Army forces generate combat power by converting*
2605 *potential into effective action (FM 3-0).* There are eight elements of combat power. The first two—
2606 leadership and information—are applied throughout and multiply the effects of the other six elements of
2607 combat power, collectively described as the Army warfighting functions. (Refer to FM 3-0, chapter 4, for a
2608 full discussion of the elements of combat power.)

- 2609 ● Movement and maneuver.
- 2610 ● Intelligence.
- 2611 ● Fires.
- 2612 ● Sustainment.
- 2613 ● C2.

FOR OFFICIAL USE ONLY

- 2614 • Protection.

2615 **ARMY CAPABILITIES**

2616 3-22. An ARFOR is the Army Service component headquarters for a JTF or a joint and multinational force
 2617 (FM 3-0). MI has responsibilities and functions that support full spectrum operations at all echelons. The
 2618 distribution of specific intelligence assets enhances the capability of the combined arms team. The planning
 2619 and analysis of force tailoring identifies intelligence resources and capabilities required and blends the
 2620 mission requirements necessary for mission success. The task organization that follows force tailoring
 2621 establishes an ordered command and support structure for the intelligence assets to conduct their support
 2622 missions.

2623 **COMBINED ARMS**

2624 3-23. Combined arms is the synchronized and simultaneous application of the elements of combat
 2625 power—to achieve an effect greater than if each element of combat power was used separately or
 2626 sequentially
 2627 (FM 3-0). As an integral part of combined arms, staffs must identify all intelligence capabilities that will be
 2628 required to conduct operations in an assigned AO. Specific units with those specific intelligence
 2629 capabilities will then be requested for the force pool for force tailoring.

2630 **FORCE TAILORING**

2631 3-24. *Force tailoring is the process of determining the right mix of forces and the sequence of their*
 2632 *deployment in support of a joint force commander* (FM 3-0). Force tailoring involves selecting the right
 2633 force structure for a joint operation from available units within a combatant command or from the Army
 2634 force pool. Based on mission analysis, the staff at each echelon identifies intelligence capabilities and
 2635 resources to support the commander’s guidance, intent, and mission objectives.

2636 **TASK-ORGANIZING**

2637 3-25. *Task-organizing is the act of designing an operating force, support staff, or logistic package of*
 2638 *specific size and composition to meet a unique task or mission. Characteristics to examine when task-*
 2639 *organizing the force include but are not limited to training, experience, equipage, sustainability, operating*
 2640 *environment, enemy threat, and mobility. For Army forces, it includes allocating available assets to*
 2641 *subordinate commanders and establishing their command and support relationships* (FM 3-0).

2642 3-26. Once intelligence assets have been allocated, each echelon task-organizes those intelligence assets to
 2643 provide maximum mission support. Task-organizing of intelligence assets occur within a tailored force
 2644 package as commanders organize units for specific missions. Intelligence assets are task-organized to force
 2645 packages based on intelligence capability requirements for each force’s mission. As commanders
 2646 reorganize units for subsequent missions, intelligence assets may be redistributed in order to support new
 2647 or changing requirements.

2648 **COMMAND AND SUPPORT RELATIONSHIPS**

2649 3-27. Command and support relationships provide the basis for unity of command in operations.
 2650 Command and relationships may limit the ability of a commander to affect task organization. Commanders
 2651 use Army command and support relationships when task-organizing MI assets. Since most MI forces are
 2652 task-organized to support operations, MI leaders at all echelons must understand the impact of command
 2653 and support relationships on their units, personnel, and assets. Command and support relationships may fall
 2654 within the framework of joint doctrine. See JP 1 for a discussion of joint command relationships and
 2655 authorities. See FM 3-0, appendix B, for a discussion of command and support relationships.

2656 3-28. Table 3-1 lists the Army command relationships and their inherent responsibilities.

FOR OFFICIAL USE ONLY

2657 3-29. While not an actual command or support relationship, technical channels often affect certain
2658 intelligence operations. Intelligence commanders and the intelligence staff maintain control of each
2659 intelligence discipline during operations through technical channels to ensure adherence to applicable laws
2660 and policies, ensure proper use of doctrinal techniques, and provide technical support and guidance.
2661 Applicable laws and policies include all relevant US law, the law of war, international law, directives,
2662 DOD Instructions, and orders. In specific cases, regulatory authority is granted to national and DOD
2663 intelligence agencies for specific intelligence discipline collection and is passed through technical
2664 channels.

2665 3-30. Commanders direct operations but often rely on technical expertise to plan, prepare, execute, and
2666 assess portions of the unit's collection effort. Technical channels also involve translating ISR tasks into the
2667 specific parameters used to focus highly technical or legally sensitive aspects of the ISR effort. Technical
2668 channels include, but are not limited to—

- 2669 ● Defining, managing, or guiding the employment of specific ISR assets.
- 2670 ● Identifying critical technical collection criteria such as technical indicators.
- 2671 ● Recommending collection techniques, procedures, or assets.
- 2672 ● Conducting operational reviews.
- 2673 ● Conducting operational coordination.
- 2674 ● Conducting specialized training for specific MI personnel or units.

2675 3-31. An example of technical channels is the Prophet control team converting the PIR and ISR tasks
2676 developed during the MDMP and assigning times and anticipated enemy frequencies for subordinate
2677 Prophet teams to collect.

2678

FOR OFFICIAL USE ONLY

2681

Chapter 4

2682

Intelligence Process in Full Spectrum Operations

2683

THE INTELLIGENCE PROCESS

2684

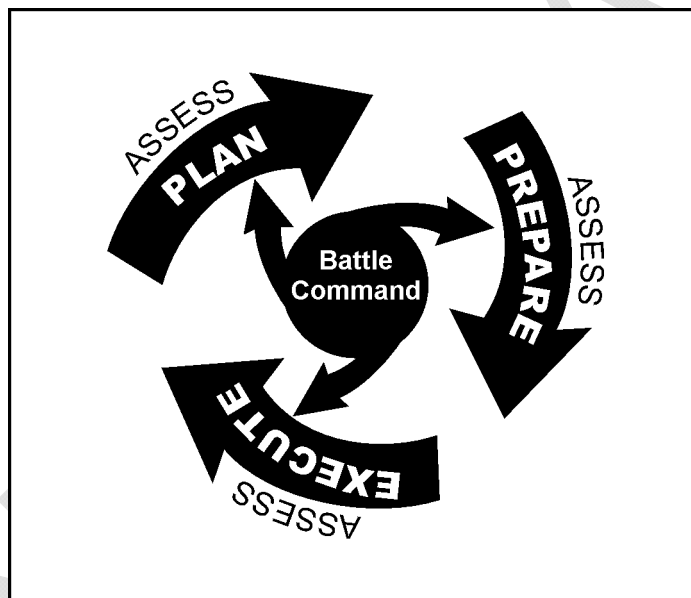
4-1. Commanders use the operations process of plan, prepare, execute, and assess to continuously design and conduct operations. Figure 4-1 shows this process. The commander cannot successfully accomplish the activities involved in the operations process without information and intelligence. The design and structure of intelligence operations support the commander's operations process by providing him with intelligence regarding the threat, terrain and weather, and civil considerations.

2685

2686

2687

2688



2689

Figure 4-1. The operations process

2690

4-2. The operations process and the intelligence process are mutually dependent. The commander provides the guidance and focus through CCIRs (PIRs and FFIRs) that drives the operations and intelligence processes. The intelligence process operates during all parts of the operations process in order to provide the continuous intelligence essential to the operations process. Intelligence about the threat, terrain and weather, and civil considerations supports Army forces in combining offensive, defensive, and stability or civil support operations simultaneously as part of an interdependent joint force to seize, retain, and exploit the initiative, accepting prudent risk to create opportunities to achieve decisive results. IPB is one of the integrating processes that occurs during all operations process activities and must be synchronized with each other as well as integrated into the overall operation. Figure 4-2 shows the relationship between the operations and intelligence processes.

2691

2692

2693

2694

2695

2696

2697

2698

2699

2700

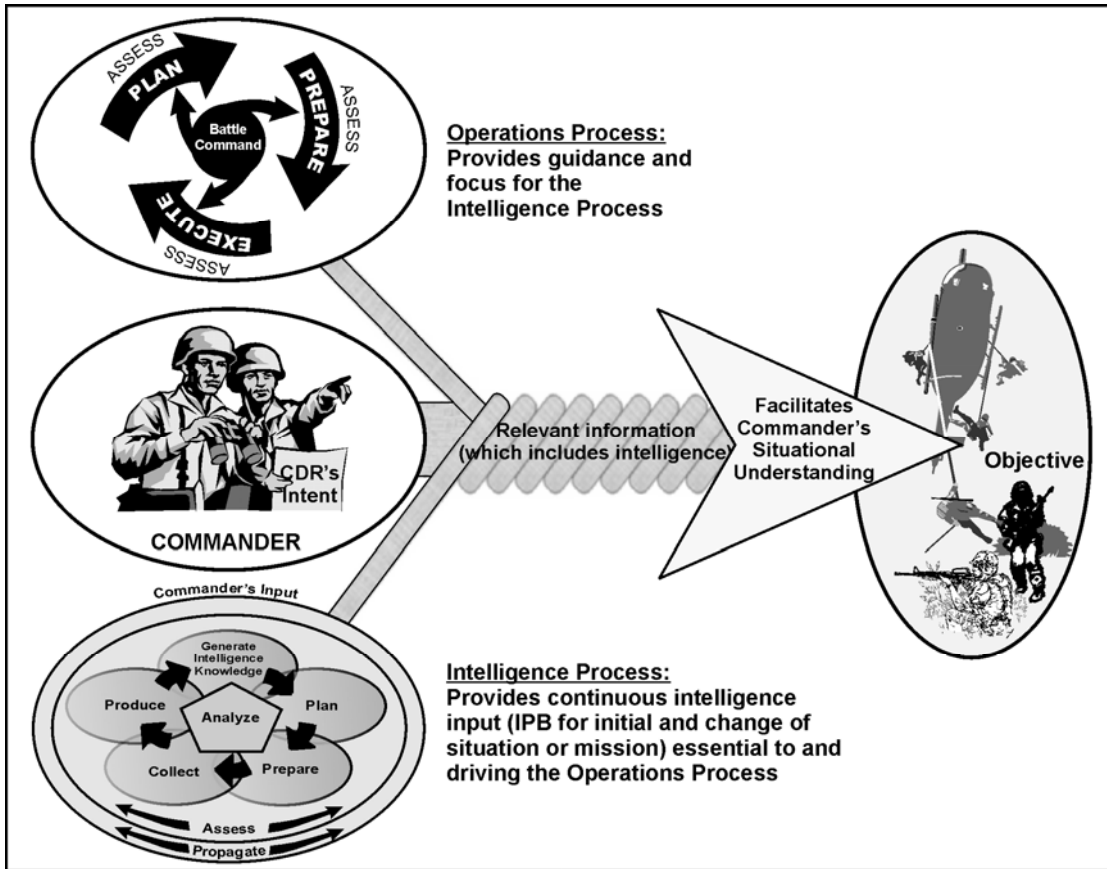
4-3. Intelligence operations consist of the five steps that constitute the intelligence process and four continuing activities. Just as the activities of the operations process overlap and recur as the mission demands, so do the steps of the intelligence process. Additionally, the analyze, commander's input, assess,

2701

2702

FOR OFFICIAL USE ONLY

2703 and propagate continuing activities of the intelligence process occur continuously throughout the
 2704 intelligence process.



2705 **Figure 4-2. The relationship between the operations and intelligence processes**

2706 **GENERATE INTELLIGENCE KNOWLEDGE**

2707 4-4. Generate intelligence knowledge consists of all activities necessary to collect the initial (baseline)
 2708 information and intelligence from existing sources in order to develop an initial intelligence survey and an
 2709 initial intelligence estimate in preparation for the MDMP with the staff. Additionally, the G-2/S-2 must
 2710 retrieve, update, or develop any required intelligence databases.

2711 4-5. The generate intelligence knowledge step of the intelligence process must be accomplished well in
 2712 advance of the mission analysis step of MDMP and prior to conducting the initial IPB. This step must be
 2713 completed thoroughly in order to prepare the intelligence staff for the planning step. It also sets the stage
 2714 for developing ISR operations. For further information on generate intelligence knowledge, see paragraph
 2715 1-56.

2716 **PLAN**

2717 4-6. The planning step of the intelligence process consists of activities that include assessing the
 2718 situation, envisioning the commander's desired endstate, identifying pertinent information and intelligence
 2719 requirements in coordination with the commander, developing an ISR plan to satisfy those requirements in
 2720 coordination with the operations officer, directing intelligence operations, and synchronizing the
 2721 intelligence effort.

FOR OFFICIAL USE ONLY

2722 4-7. The G-2/S-2 must ensure that they are working closely with the G-3/S-3 on the ISR plan and that
 2723 both are working from the same intelligence baseline. The commander’s intent, planning guidance, and
 2724 CCIRs (PIRs and FFIRs) drive the planning of intelligence operations. Planning, managing, and
 2725 coordinating these operations are continuous activities necessary to obtain information and produce
 2726 intelligence essential to decision making.

2727 **Coordinate**

2728 4-8. Staff and leaders coordinate with various organizations to ensure the necessary resources, such as
 2729 linguist support (see appendix B), information, intelligence, training, and procedures are in place to
 2730 facilitate effective intelligence operations.

- 2731 ● Coordination for and Management for Movement of ISR Assets. All ISR assets at one time or
 2732 another will move through or near another unit’s AO. To avoid fratricide, ISR elements must
 2733 coordinate with units, G-3/S-3, G-2/S-2, and each other, ISR elements must also coordinate with
 2734 appropriate staff elements to establish no-fire areas and/or other fire support coordination
 2735 measures around ISR assets, airspace control measures, and appropriate weapons control status
 2736 (in reference to aerial ISR assets).
- 2737 ● Coordination for and Management of Information and Intelligence. The intelligence staff must
 2738 prepare and practice coordination and management with personnel from all MI units, non-MI
 2739 units, other Service components, and multinational organizations that may contribute to or
 2740 facilitate the ISR effort. This coordination enables the G-2/S-2 to share and update databases,
 2741 information, and intelligence and ensures connectivity with those organizations. All units are
 2742 sources of relevant information regarding the enemy and the operational environment.
- 2743 ● Liaison. In order to accomplish the mission, exchange information and intelligence, move
 2744 through certain areas and ensure protection, it may be necessary to coordinate with many
 2745 different elements, organizations, and LNs of the country in which friendly forces are
 2746 conducting operations. LNs include police, town officials, foreign military forces, and political
 2747 and other key figures within the AO. Operations may also necessitate coordination with other
 2748 US and multinational forces; for example, the International Security Assistance Force, the
 2749 International Police Task Force, Organization for Security and Cooperation in Europe, and
 2750 Defense HUMINT.
- 2751 ● Movement. Coordination with the G-3/S-3 and proper management ensures ease of movement
 2752 and safe passage of friendly forces through an area. Coordinating movement also helps avoid
 2753 fratricide.

2754 **Planning Considerations for Intelligence Warfighting Function**

2755 4-9. The intelligence warfighting function is a unified system that anticipates and satisfies intelligence
 2756 needs. Commanders ensure its proper employment by clearly articulating intent, designating CCIRs (PIRs
 2757 and FFIRs), and prioritizing targets. Commanders must, however, understand the limitations of the
 2758 intelligence warfighting function to preclude unrealistic expectations of the system. The following are
 2759 intelligence warfighting function considerations:

- 2760 ● Intelligence only reduces uncertainty in the AO; it does not eliminate it entirely. The commander
 2761 will always have to determine the presence and degree of risk involved in conducting a
 2762 particular mission.
- 2763 ● The intelligence warfighting function is composed of finite resources and capabilities.
 2764 Intelligence systems and Soldiers trained in specific ISR skills are limited in any unit. Once lost
 2765 to action or accident, these Soldiers and systems are not easily replaceable; for some, it may not
 2766 be possible to replace them during the course of the current operation. The loss of Soldiers and
 2767 equipment can result in the inability to detect or analyze enemy actions. The loss of qualified
 2768 language-trained Soldiers, especially Soldiers trained in low-density languages or skills, could
 2769 adversely affect intelligence operations as well.

FOR OFFICIAL USE ONLY

- 2770
- 2771
- 2772
- 2773
- 2774
- 2775
- 2776
- 2777
- 2778
- 2779
- 2780
- 2781
- 2782
- In order to effectively and efficiently provide timely, relevant, accurate, predictive, and tailored intelligence, the intelligence warfighting function must have adequate communications equipment, capacity, and connectivity. Commanders and G-2/S-2s must ensure communications support to intelligence has the appropriate priority.
 - Commanders and G-2/S-2s cannot expect that higher echelons will automatically send them everything they need. While intelligence reach is a valuable tool, the push of intelligence products from higher echelons does not relieve subordinate staffs from conducting detailed analysis and focusing the efforts of higher headquarters. Nor can they expect products pushed to them to be always at the level of detail they require. Utilizing the DCGS-A enterprise, commanders and G-2/S-2s must focus higher echelons by clearly articulating and actively pursuing intelligence requirements. By providing higher echelons with a clear picture of the required intelligence products, commanders can also narrow the flow of intelligence and information and preclude being overwhelmed by too much information.

2783

2784

2785

2786

2787

4-10. Commanders should be aware that intelligence collection is enabled by, and subject to, laws, regulations, and policies to ensure proper conduct of intelligence operations. While there are too many to list here specifically, categories of these legal considerations include United States Codes, Executive Orders, National Security Council Intelligence Directives, Army Regulations, United States Signal Intelligence Directives, SOFAs, ROE, and other international laws and directives.

2788

Red Teaming

2789

2790

2791

2792

2793

2794

4-11. Whenever possible, commanders employ red teams to examine plans from a threat's perspective. Red team is a special staff section whose members primarily participate in planning in the future operations and plans cells unless integrated into another cell. Red team members anticipate cultural perception of partners, enemies, adversaries, and others, and conducts independent critical reviews and analysis. The red team provides the commander with an enhanced capability to explore alternatives during planning and execution.

2795

2796

2797

2798

2799

4-12. Red teaming provides commanders alternative perspectives by challenging planning assumptions, assisting in defining the problem and end-state, identifying friendly and enemy vulnerabilities, and identifying assessment measures. These alternative perspectives not only account for the threat and environment in plans, concepts, organizations, and capabilities but also address the standpoint of our multinational partners, enemies, and adversaries, and other perspectives.

2800

ISR Planning Considerations

2801

2802

2803

2804

2805

2806

2807

2808

4-13. ISR planning consists of two significant staff processes: ISR synchronization and ISR integration. ISR synchronization is the responsibility of the intelligence officer and the G-2/S-2 staff. The operations officer is responsible for ISR integration with the support of the intelligence officer. ISR synchronization involves the entire staff and all of the warfighting functions. All staff sections within a command post have the responsibility to satisfy information requirements. Satisfying information requirements through staff element coordination facilitates ISR planning by eliminating the necessity to task an asset to collect information that another unit or asset already observed in the course of operations. The commander may designate an ISR working group; however, the primary staff's responsibilities cannot be delegated.

2809

2810

2811

4-14. When planning, preparing, conducting, and assessing ISR operations, the intelligence staff must strive to achieve maximum efficiency and effectiveness. The intelligence staff considers six essential criteria in conducting ISR synchronization for the following:

- 2812
- 2813
- 2814
- 2815
- 2816
- **Anticipate.** The intelligence officer must recognize when and where to shift collection or identify new intelligence requirements. The intent of this principle is to identify a new or adjust an existing requirement and present it to the commander before the commander or other staff members identify the need. By participating in the decision making, planning, and operations processes, intelligence officers can best anticipate requirements.

FOR OFFICIAL USE ONLY

- 2817 ● **Coordinate.** The intelligence staff must coordinate and collaborate with all staff sections and
2818 with both higher headquarters, subordinate, and adjacent units in order for ISR operations to be
2819 continuously synchronized. The intelligence staff must be engaged in the unit’s planning and
2820 orders production activities to ensure early identification of intelligence requirements. The
2821 intelligence staff must also be integrated into the combat information reporting and battle
2822 tracking of current operations to anticipate the need for dynamic or ad hoc ISR taskings. Early
2823 and continuous consideration of ISR planning factors enhances the unit’s ability to direct ISR
2824 assets in a timely manner in support of developing situations, ensures thorough planning, and
2825 increases flexibility in selecting and retasking assets.
 - 2826 ● **Prioritize.** The priority for ISR operations begins with the CCIR. Then intelligence officers
2827 prioritize each validated intelligence requirement based upon its importance in supporting the
2828 commander’s intent and decisions and the current situation so that low-density and high-demand
2829 ISR assets and resources are directed against the most critical requirements.
 - 2830 ● **Balance.** Balance involves using a combination of redundancy, mix, and cueing of a variety of
2831 ISR capabilities to complement each other. Balance is simply achieving maximum efficiency
2832 using an appropriate mix of disciplines, ISR assets, and resources to satisfy as many competing
2833 intelligence requirements as possible.
 - 2834 ■ *Redundancy* is achieved using several same-type ISR assets to cover the same named area
2835 of interest (NAI).
 - 2836 ■ *Mix* means planning for complementary coverage by a combination of assets from multiple
2837 units and intelligence disciplines designed to increase the probability of collection success
2838 and reduce the chances of successful threat deception.
 - 2839 ■ *Cueing* involves the use of one or more sensors to provide data that result in another system
2840 to conducting collection. Balance also means that the intelligence staff should resist
2841 favoring or becoming too reliant on one particular unit, discipline, or system.
 - 2842 ● **Control.** Units should first use organic and allocated ISR assets to ensure timely and effective
2843 collection as well as overall synchronization. These assets are more responsive to the
2844 commander’s needs and can be balanced with other resources. ISR assets belonging other units,
2845 agencies, or organizations may have limited availability and are likely to receive differing
2846 priorities from their respective commanders. Information gathered by other ISR resources is
2847 harder to verify and correlate with information collected by organic assets.
 - 2848 ● **Reach.** Units can use intelligence reach and RFIs to answer initial information requirements
2849 without having to use the echelon’s ISR assets. Intelligence which is confirmed by more than
2850 one intelligence discipline is generally preferred over single-source reporting. Therefore, a unit
2851 should not depend solely on intelligence reach to satisfy a PIR.
- 2852 4-15. The staff must not only carefully focus ISR plans on answering the CCIRs (PIRs and FFIRs) but also
2853 enable the quick retasking of units and assets as the situation changes. ISR synchronization includes
2854 continually identifying new and partially filled intelligence gaps. This ensures that the developing threat
2855 situation, not just our OPLAN, “drives” ISR operations. Specifically, intelligence officers—
- 2856 ● Evaluate ISR assets for suitability (availability, capability, vulnerability, and performance
2857 history) to execute ISR tasks and make appropriate recommendations on asset tasking to the
2858 operations officer.
 - 2859 ● Assess ISR collection against CCIRs (PIRs and FFIRs) to determine the effectiveness of the ISR
2860 plan. They maintain situational awareness in order to identify gaps in coverage and to identify
2861 the need to cue or recommend redirecting ISR assets to the operations officer,
 - 2862 ● Update the ISR synchronization plan as requirements are satisfied modified, or created. They
2863 remove satisfied requirements and recommend new requirements as necessary.
 - 2864 ● In coordination with operations staff, monitor satisfactory completion of ISR tasks from higher
2865 headquarters. Operations officer integrate the updated synchronization plan into orders tasking
2866 ISR assets.

FOR OFFICIAL USE ONLY

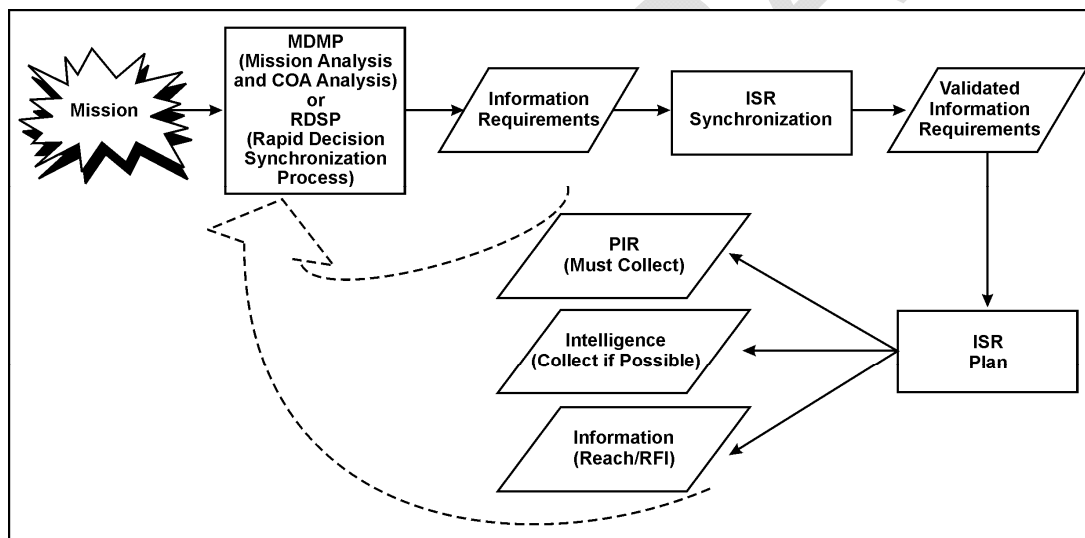
2867 4-16. ISR operations require constant coordination between the current operations, intelligence, and plans
 2868 cells within an organization. The entire staff participates in ISR planning. The G-2S-2 is the lead for ISR
 2869 synchronization. The G-3/S-3 creates the ISR plan.

2870 4-17. ISR integration is vital in controlling limited ISR assets. Thoroughly integrated ISR operations add
 2871 many collection resources, multiplying the potential for multi-source collection of information. The
 2872 ongoing activities of ISR all contribute to updating the ISR plan.

2873 4-18. FMI 2-01 describes the ISR synchronization process in detail. FM 3-55 (when published) will
 2874 address ISR overall.

2875 Requirements

2876 4-19. For intelligence purposes there are three types of requirements: PIRs, intelligence requirements, and
 2877 information requirements. Each requirement is broken down into discrete pieces to answer that
 2878 requirement. These pieces are referred to as indicators and specific information requirements, which
 2879 facilitate the answering of the requirements. The indicators and specific information requirements are used
 2880 by ISR planners to develop the ISR plan. Figure 4-3 shows the process of developing requirements and
 2881 integrating them into the ISR process.



2882 **Figure 4-3. Requirements development and integration into the ISR process**

2883 *Commander's Critical Information Requirement*

2884 4-20. A commander's critical information requirement is an information requirement identified by the
 2885 commander as being critical to facilitating timely decision making. The two key elements are friendly force
 2886 information requirements and priority intelligence requirements (JP 3-0).

2887 4-21. A CCIR directly influences decision making and facilitates the successful execution of military
 2888 operations. Commanders decide whether to designate an information requirement as a CCIR based on
 2889 likely decisions and their visualization of the COA. A CCIR may support one or more decisions. The list of
 2890 CCIRs constantly changes. Commanders add and delete individual requirements throughout an operation
 2891 based on the information needed for specific decisions.

FOR OFFICIAL USE ONLY

2892 *Validated Information Requirements*

2893 4-22. There are three types of validated information requirements that result from ISR synchronization:
2894 PIRs, intelligence requirements, and information requirements.

- 2895 ● **Priority Intelligence Requirements.** A priority intelligence requirement is an intelligence
2896 requirement, stated by the commander as a priority for intelligence support which the
2897 commander needs to support decision making and to understand the AO or the threat. The
2898 intelligence officer manages PIRs for the commander, but the PIRs belong solely to the
2899 commander. All staff sections may recommend requirements that may become PIRs. PIRs are
2900 selected as part of the process of identifying CCIRs during mission analysis; they, along with
2901 friendly force information requirements (FFIRs), are updated as part of updating the CCIRs
2902 throughout the operation. PIRs have first priority in collection assets tasked to their collection.
- 2903 ● **Intelligence Requirements.** An intelligence requirement is a type of information requirement
2904 developed by subordinate commanders and the staff (to include subordinate staffs) that requires
2905 dedicated ISR collection for the elements of threat, terrain and weather, and civil
2906 considerations. Intelligence requirements are developed by the staff and subordinate
2907 commanders (and their staffs) and must be answered to facilitate operations. They require ISR
2908 collection assets to be assigned for their collection, second in priority to PIRs.
- 2909 ● **Information Requirements.** Information requirements are all information elements the
2910 commander and staff require to successfully conduct operations; that is, all elements necessary
2911 to address the factors of METT-TC (FM 6-0). After validated requirements are identified and
2912 the ISR plan is completed, there may additional information requirements that support the
2913 development of situational understanding, answer gaps in the COP, and provide additional
2914 details required for analysis. These are information requirements that do not require collection
2915 by ISR assets to be answered. The staff answers these requirements through intelligence reach or
2916 RFIs.

2917 **PREPARE**

2918 4-23. The best plans will not ensure success without meticulous and thorough preparation for operations.
2919 The prepare task includes those staff and leader activities which take place upon receiving the OPORD,
2920 OPLAN, WARNO, or commander's intent to improve the unit's ability to execute tasks or missions and
2921 survive on the battlefield. For intelligence units, these activities include—

- 2922 ● Conducting necessary coordination in accordance with the OPORD, METT-TC, unit SOP.
- 2923 ● Establishing and testing the intelligence architecture. This activity includes complex and
2924 technical issues like hardware, software, communications, COMSEC materials, network
2925 classification, technicians, database access, LNOs, training, funding, and TTP.
- 2926 ● Establishing intelligence team cohesiveness. This activity includes knowing different unit's and
2927 organization's capabilities, training the necessary collective skills, establishing effective
2928 relationships with different units and organizations, developing mutual battle rhythms and TTP,
2929 and leveraging the right architectures and collaboration tools.
- 2930 ● Coordinating effective analytic collaboration. This activity is necessary to maximize the
2931 complementary analytic capabilities of different units and organizations that produce
2932 intelligence within the same JOA. Coordinating this collaboration is an effort-intensive activity
2933 that requires careful mutual planning, division of labor, defined responsibilities, and procedures
2934 for adapting to changing circumstances as they develop.
- 2935 ● Establishing reporting procedures.
- 2936 ● Updating IPB, the intelligence running estimate, and ISR synchronization.
- 2937 ● Producing intelligence estimates.
- 2938 ● Ensuring staff and personnel are trained. If personnel are not adequately trained at this point,
2939 they must be trained or the leader must evaluate the risk they bring to the operation.

FOR OFFICIAL USE ONLY

- 2940 ● Planning refinement, brief-backs, SOP reviews, and rehearsals, and coordinating with various
2941 elements and organizations.
- 2942 ● Establishing other troop-leading procedures or coordination, as necessary, in accordance with
2943 METT-TC factors.

2944 **G-2/S-2 Preparation Activities**

- 2945 4-24. The G-2/S-2 takes numerous steps before mission execution to ensure intelligence operations run
2946 smoothly and effectively within the staff section. These steps include, but are not limited to, the following:
- 2947 ● Conduct rehearsals (at a minimum communications, intelligence production, ISR, and unit
2948 rehearsals).
- 2949 ● Review and update available databases and IPB products.
- 2950 ● Review applicable SOPs, Army Regulations, DA Pamphlets, Field Manuals, and ROE for
2951 guidance in conducting intelligence operations.
- 2952 ● Plan and practice actions supporting likely contingencies, or the branches or sequels to an
2953 operation.
- 2954 ● Verify coordination measures are still in effect.
- 2955 ● Conduct essential training (individual and collective) that is realistic and tied to the mission.
- 2956 ● Verify communications protocols with theater and higher headquarters and subordinate and
2957 lateral units.
- 2958 ● Update intelligence databases.
- 2959 ● Update the forces with the most recent intelligence on the AO immediately before mission
2960 execution.

2961 **Inspections**

- 2962 4-25. Once all required equipment and support materials have been acquired, staff and leaders must
2963 conduct inspections to ensure that the unit and Soldiers are prepared to conduct their mission. It is crucial
2964 that staff and leaders check to verify that procedures, personnel, equipment, and services are in place and
2965 ready for mission execution. Leaders can only expect what they inspect.

2966 **Rehearsals**

- 2967 4-26. Rehearsals help units prepare for operations by either verifying that provisions and procedures are in
2968 place and functioning or identifying inadequacies, which staff and leaders must remedy. They allow
2969 participants in an operation to become familiar with and to translate the plan into specific actions that
2970 orient them to their environment and other units when executing the mission. They also imprint a mental
2971 picture of the sequence of key actions within the operation and provide a forum for subordinate and
2972 supporting leaders and units to coordinate.

2973 **Communications**

- 2974 4-27. Staff and leaders must work closely with the G-6/S-6 to coordinate for the required communication
2975 links. The unit may require classified and unclassified network connections for their equipment. If
2976 elements of the unit will be working outside the range of the unit's communications systems, then it is
2977 necessary to coordinate for global or extended range communications. Leaders must obtain the required
2978 type and amount of communications equipment and related components as well as the latest fills and
2979 frequencies. They must possess and be familiar with all the instructions, passwords, policies, regulations,
2980 and directives conducive to OPSEC. They must also ensure Soldiers are trained in the use and procedures
2981 involved in operating communications equipment. The G-2/S-2 must verify the frequencies, alternate
2982 frequencies, and reactions during jamming, as well as the latest time information is of value (LTIOV) for
2983 specific information to be reported.

FOR OFFICIAL USE ONLY

2984 **Situation Updates**

2985 4-28. Staff preparation includes assembling and continuously updating estimates. For example, continuous
 2986 IPB provides accurate situational updates for commanders. The G-2/S-2 operations team uses the DCGS-A
 2987 enterprise and automated tools to continuously integrate information and intelligence products from
 2988 subordinate G-2/S-2s and supporting ISR organizations to update the threat situation, terrain and weather,
 2989 and civil considerations.

2990 **Intelligence Handoff**

2991 4-29. Intelligence handoff may occur in three primary situations: Intelligence handoff when handing over a
 2992 mission (during relief in place/transition of authority), when handing off targets, or when handing off
 2993 technical channels for intelligence assets. A well-prepared intelligence handoff will ensure a smooth and
 2994 seamless transition between units. It is important that the receiving unit becomes familiar with the
 2995 operation, target, or technical channels requirements as soon as possible to avoid compromising the
 2996 intelligence production and flow of the mission. The following are points to consider during an intelligence
 2997 handoff:

- 2998 ● Briefings and reports (learn what briefings are required and when, as well as report formats and
 2999 requirements—to include technical requirements).
- 3000 ● Past, present, and planned activities within the area of influence.
- 3001 ● Established SOPs (know procedures for reporting; intelligence contingency funds and incentive
 3002 use if applicable; emplacement and use of ISR equipment).
- 3003 ● Key personalities (introductions are required; establish rapport and a good working relationship
 3004 with all key personalities).
- 3005 ● Key personnel on the base or camp (their responsibilities; how to contact them).
- 3006 ● Key personnel in other US and multinational service components (coordinate for exchange of
 3007 information and intelligence).
- 3008 ● Key personalities from surrounding towns (local figures).
- 3009 ● Key national level political and military figures.
- 3010 ● Supporting units (know where to go for sustainment, information, or assistance and POCs
 3011 within those organizations).
- 3012 ● Current attitudes (understand current attitudes and perspectives of the local populace).
- 3013 ● Equipment operation and idiosyncrasies (equipment may run on different applications;
 3014 personnel may need to train on specific equipment and procedures).
- 3015 ● Area familiarization (identify NAIs, key terrain, minefields, and boundaries; know camp
 3016 locations, routes and route names, checkpoints, and towns).
- 3017 ● Handover of databases; for example, analytical, intelligence discipline databases, source
 3018 registry, technical channels, and POCs.
- 3019 ● Close coordination for cross-boundary target handoff ; for example, complete target information
 3020 (when not handing off a formal target package) on a target which conducts cross-boundary
 3021 operations.
- 3022 ● The specific aspects of technical channels.

3023 **Rules of Engagement**

3024 4-30. Although ROE training was presented during the plan step of the intelligence process, leaders at all
 3025 levels can take the opportunity during the prepare step to ensure their subordinates completely understand
 3026 the ROE. During this step commanders may need to consider exceptions to, or modifications of, the ROE
 3027 to facilitate HUMINT and CI collection or to enable the placement of ISR assets.

FOR OFFICIAL USE ONLY

3028 **COLLECT**

3029 4-31. The G-2/S-2 and G-3/S-3 play a critical role in this challenging step because intelligence drives
3030 operations. Elements of all units in the AO obtain information and data about the threat, terrain and
3031 weather, and civil considerations in the AO. Well-developed procedures and carefully planned flexibility to
3032 support emerging targets, changing requirements, and the need to support combat assessment is critical.
3033 Once the information has been collected, it must be processed into a form that enables analysts to extract
3034 essential information and produce intelligence and targeting data. Collected and processed information
3035 must then be reported to the appropriate units, organizations, or agencies for analysis or action.

3036 **ISR Tasks and Other Intelligence-Related Tasks**

3037 4-32. ISR synchronization and integration results in an effort focused on answering the CCIR through ISR
3038 tasks translated into orders. ISR assets must be focused properly to collect the knowledge the commander
3039 needs at the right time in order to achieve mission success. Successful ISR operations allow commanders to
3040 engage the threat through knowledge rather than assumptions.

3041 4-33. Intelligence tasks are included in annex B of the OPORD under Scheme of Intelligence. They
3042 include the following:

- 3043 • **Intelligence Production.** Intelligence production includes analyzing information and
3044 intelligence and presenting intelligence products, conclusions, or projections regarding the
3045 operational environment and enemy forces in a format that enables the commander to achieve
3046 situational understanding.
- 3047 • **Request for Information.** Submitting an RFI to the next higher headquarters or adjacent units
3048 is the normal procedure for obtaining intelligence information not available through the use of
3049 available ISR assets. Users enter RFIs into an RFI management system where every other user
3050 of that system can see it. Hence, an echelon several echelons above the actual requester becomes
3051 aware of the request and may be able to answer it. A G-2/S-2 who receives an RFI from a
3052 subordinate element may use intelligence reach to answer RFIs.
- 3053 • **Intelligence Reach.** Intelligence reach allows the commander to access the resources of
3054 national, joint, foreign, and other military organizations and units. Requestors can acquire
3055 information through push and pull of information, databases, homepages, collaborative tools,
3056 and broadcast services. Intelligence reach also supports distributed analysis. (See chapter 2 for
3057 more information on intelligence reach.)

3058 4-34. For information on surveillance and reconnaissance tasks, refer to FM 3-55 (when published) and
3059 FM 7-15 (when published).

3060 **Special Reconnaissance**

3061 4-35. Special reconnaissance is the complementing of national and theater intelligence collection assets
3062 and systems by obtaining specific, well-defined, and time-sensitive information of strategic or operational
3063 significance. It may complement other collection methods where there are constraints of weather, terrain,
3064 hostile countermeasures, and/or other systems availability. Special reconnaissance places US or US-
3065 controlled personnel conducting direct observation in hostile, denied, or politically sensitive territory when
3066 authorized. SOF may conduct these missions unilaterally or in support of conventional operations. (See
3067 JP 3-05.)

3068 4-36. Army Special Operations Forces elements conduct special reconnaissance missions to obtain
3069 information not available through other means. Special reconnaissance operations encompass a broad
3070 range of collection activities to include surveillance, reconnaissance, and target acquisition. Special
3071 reconnaissance missions provide intelligence or information that is often not available through other
3072 means. Typical special reconnaissance missions include—

FOR OFFICIAL USE ONLY

- 3073 ● Surveillance and target acquisition of hostile C2 systems, troop concentrations, deep-strike
3074 weapons, lines of communication, CBRNE capabilities, and other targets.
- 3075 ● Location and surveillance of hostage, enemy prisoner of war (EPW), or political prisoner
3076 detention facilities.
- 3077 ● Post-strike reconnaissance for BDA.
- 3078 ● Meteorologic, geographic, or hydrographic reconnaissance to support specific air, land, or sea
3079 operations.

3080 4-37. For more information on special reconnaissance, see FM 3-05.102.

3081 **Process**

3082 4-38. Processing converts relevant information into a form suitable for analysis, production, or immediate
3083 use by the commander. Processing includes sorting through large amounts of collected information and
3084 intelligence (multidiscipline reports from the unit's ISR assets, adjacent and higher echelon units and
3085 organizations, and non-MI elements in the AO). Processing identifies and exploits that information which
3086 is pertinent to the commander's intelligence requirements and facilitates situational understanding.
3087 Examples of processing include enhancing imagery, translating a document from a foreign language,
3088 converting electronic data into a standardized report that can be analyzed by a system operator, and
3089 correlating dissimilar or jumbled information by assembling like elements before the information is
3090 forwarded for analysis.

3091 4-39. Often collection assets must collect and process their data prior to disseminating it. MI systems have
3092 their own reporting and processing systems, the details of which are in the appropriate MI system manuals
3093 and technical manuals. Some collection assets, particularly air reconnaissance and ground scouts, can
3094 report relevant information that is immediately usable by the tactical commander (for example, for
3095 targeting purposes). However, the personnel in the reporting chain still process these reports by evaluating
3096 their relevancy and accuracy. In many cases, the output of a collection asset is data, or information of
3097 limited immediate use to a commander.

3098 4-40. The intelligence staff processes information collected by the unit's assets as well as that received
3099 from higher echelons. Through intelligence reach, the intelligence staff processes many types of
3100 information and data from all of the intelligence disciplines and from both the unit's ISR assets and from
3101 ISR assets outside the unit.

3102 **Reporting**

3103 4-41. The most critical information collected is worthless if not reported in a timely manner. Collectors
3104 may report information via verbal, written, graphic, or electronic means. Unit SOPs must clearly state the
3105 transmission means of different types of reports (for example, sent by satellite communications, FM radios,
3106 or by automated means). In general, the transmission of reports for threat contact and actions, CCIRs,
3107 exceptional information, and CBRNE reports is by voice FM, and then followed up with automated
3108 reports.

3109 4-42. Commanders and staffs must remember that timely reporting, especially of threat activity, is critical
3110 in fast-moving operations. Collectors must report accurate information as quickly as possible. Commanders
3111 and staff must not delay reports for the sole purpose of editing and ensuring the correct format. This is
3112 particularly true for reporting information or intelligence that answers the CCIR.

3113 4-43. The G-2/S-2 coordinates with the unit staff, subordinate and lateral commands, and higher echelon
3114 units to ensure that specific reporting assets, personnel, equipment (especially communications), and
3115 procedures are in place. The G-2/S-2 requests or establishes the appropriate message addresses, routing
3116 indicators, mailing addresses, and special security office security accreditation for units.

FOR OFFICIAL USE ONLY

3117 **Time-Sensitive Reporting**

3118 4-44. Intelligence and time-sensitive combat information that affects the current operation is disseminated
3119 immediately upon recognition. Combat information is unevaluated data gathered by or provided directly to
3120 the tactical commander which, due to its highly perishable nature or the criticality of the situation, cannot
3121 be processed into intelligence in time to satisfy the user's intelligence requirements. The routing of combat
3122 information proceeds immediately in two directions: directly to the commander and through routine
3123 reporting channels, which include intelligence analysis and production elements. Time-sensitive
3124 information usually includes reports concerning threat contact and actions and CCIRs.

3125 **PRODUCE**

3126 4-45. In the production task, the G-2/S-2 integrates evaluated, analyzed, and interpreted information from
3127 single or multiple sources and disciplines into finished intelligence products. Like collection operations, the
3128 G-2/S-2 must ensure the unit's information processing and intelligence production are prioritized and
3129 synchronized to support answering the CCIRs (PIRs and FFIRs).

3130 4-46. Intelligence products must be timely, relevant, accurate, predictive, and tailored. The accuracy and
3131 detail of every intelligence product has a direct effect on how well the unit conducts operations. However,
3132 the G-2/S-2 and unit must use intelligence (no matter what form the intelligence is in) that meets the
3133 requirements but might not be as detailed or refined as possible. A good answer on time is better than a
3134 more refined answer that is late.

3135 4-47. The G-2/S-2 produces intelligence for the commander as part of a collaborative process. The
3136 commander drives the G-2/S-2's intelligence production effort by establishing intelligence and information
3137 requirements with clearly defined goals and criteria. Differing unit missions and operational environments
3138 dictate numerous and varied production requirements on the G-2/S-2 and staff. Through the ISR
3139 synchronization matrix the G-2/S-2 synchronizes the information, intelligence, and PIRs with the
3140 operational timeline.

3141 4-48. The G-2/S-2 must employ collaborative analysis techniques and procedures that leverage intelligence
3142 production capability of higher and subordinate echelons to meet these requirements. Proficiency in these
3143 techniques and procedures enables the G-2/S-2 to answer the commander's and staff's requirements
3144 regardless of the mission, environment, and situation. The G-2/S-2 and staff intelligence products enable
3145 the commander to—

- 3146 ● Plan operations and employ maneuver forces effectively.
- 3147 ● Recognize potential COAs.
- 3148 ● Conduct mission preparation.
- 3149 ● Employ effective TTP.
- 3150 ● Take appropriate security measures.
- 3151 ● Focus ISR.
- 3152 ● Conduct effective targeting.
- 3153 ● Conduct assessment of intelligence and operations.

3154 **INTELLIGENCE PROCESS CONTINUING ACTIVITIES**

3155 4-49. The three continuing activities drive, shape, and develop the intelligence process. They can occur at
3156 any time during the process and help to focus and refine both the process and the intelligence products that
3157 result.

3158 **Analyze**

3159 4-50. Analysis occurs at various stages throughout the intelligence process. Leaders at all levels conduct
3160 analysis to assist in making many types of decisions. An example is a HUMINT collector's analyzing an

FOR OFFICIAL USE ONLY

- 3161 intelligence requirement in order to determine the best possible collection strategy to use against a specific
3162 source.
- 3163 4-51. Analysis in requirements management is critical to ensuring the information requirements receive the
3164 appropriate priority for collection. The intelligence staff analyzes each requirement—
- 3165 ● To determine its feasibility, whether or not it supports the commander’s intent.
 - 3166 ● To determine the best method of satisfying the information requirements.
 - 3167 ● To determine if the collected information satisfies requirements.
- 3168 4-52. During the produce task, the intelligence staff analyzes information from multiple sources to develop
3169 all-source intelligence products. The intelligence staff analyzes information and intelligence to ensure the
3170 focus, prioritization, and synchronization of the unit’s intelligence production is in accordance with the
3171 PIRs.
- 3172 4-53. In situation development, the intelligence staff analyzes information to determine its significance
3173 relative to predicted threat COAs and the CCIRs (PIRs and FFIRs). Through predictive analysis, the staff
3174 attempts to identify enemy activity or trends that represent opportunities or risks to the friendly force. They
3175 use the indicators developed for each threat COA and CCIRs (PIRs and FFIRs) during the MDMP as the
3176 basis for their analysis and conclusions.
- 3177 **Assess**
- 3178 4-54. *Assessment is the continuous monitoring and evaluation of the current situation, particularly the*
3179 *enemy, and progress of an operation* (FM 3-0). Assessment plays an integral role in all aspects of the
3180 intelligence process. Assessing the situation and available information begins upon receipt of the mission
3181 and continues throughout the intelligence process. The continual assessment of intelligence operations and
3182 ISR assets, available information and intelligence, the various aspects of the AO, are critical to—
- 3183 ● Ensure the CCIRs (PIRs and FFIRs) are answered.
 - 3184 ● Ensure intelligence requirements are met.
 - 3185 ● Redirect collection assets to support changing requirements.
 - 3186 ● Ensure operations run effectively and efficiently.
 - 3187 ● Ensure proper use of information and intelligence.
 - 3188 ● Identify enemy efforts at deception and denial.
- 3189 4-55. During planning, the intelligence staff conducts a quick initial assessment of the unit’s intelligence
3190 posture and holdings, status of intelligence estimates, and any other available intelligence products. From
3191 this assessment the commander issues his initial guidance and a WARNO.
- 3192 4-56. During execution the intelligence staff continues assessing the effectiveness of the ISR effort while
3193 at the same time assessing the results and products derived from the ISR synchronization effort. The
3194 critical aspects of assessment include determining whether—
- 3195 ● The CCIRs have been answered.
 - 3196 ● The CCIRs are still likely to be answered with the current ISR operations.
 - 3197 ● ISR operations account for changes to the CCIR.
 - 3198 ● ISR operations account for changes to the operational environment.
 - 3199 ● Some ISR operations must be adjusted in order to answer the CCIRs.
- 3200 4-57. This type of assessment requires sound judgment and a thorough knowledge of friendly military
3201 operations, characteristics of the AO and AOI, and the threat situation, doctrine, patterns, and projected
3202 COAs.

FOR OFFICIAL USE ONLY

3203 **Propagate**

3204 4-58. Successful operations at all levels require increased demands on the intelligence warfighting
 3205 function. Timely and accurate dissemination of intelligence is key to the success of operations.
 3206 Commanders must receive combat information and intelligence products in time and in an appropriate
 3207 format to support decision making. Additionally, sharing the most current all-source information and
 3208 intelligence at all echelons is essential for commanders to maintain situational understanding. The DCGS-
 3209 A enterprise is the primary method for providing intelligence products to users.

3210 4-59. To achieve this, the commander and staff must establish and support a seamless intelligence
 3211 architecture—including an effective dissemination plan—across all echelons to ensure information and
 3212 intelligence flow efficiently to all those who need them. Intelligence and communications systems continue
 3213 to evolve in their sophistication, application of technology, and accessibility to the commander. Their
 3214 increasing capabilities also create an unprecedented volume of information available to commanders at all
 3215 echelons. The commander and staff must have a basic understanding of these systems and how they
 3216 contribute to the intelligence warfighting function.

3217 **Dissemination**

3218 4-60. A dissemination plan can be a separate product, or integrated into existing products such as the ISR
 3219 synchronization plan or intelligence synchronization matrix, the decision support template, or decision
 3220 support matrix.

- 3221 ● **Dissemination Methods and Techniques.** There are numerous methods and techniques for
 3222 disseminating information and intelligence. The appropriate technique in any particular situation
 3223 depends on many factors such as capabilities and mission requirements. Possible dissemination
 3224 methods and techniques include direct electronic dissemination (a messaging program);
 3225 dissemination via chat rooms; instant messaging; web posting; printing the information and
 3226 sending it via courier; or putting the information on a compact disc and sending it to the
 3227 recipient. G-2/S-2s must plan methods and techniques to disseminate information and
 3228 intelligence when the normal methods and techniques are unavailable. For example, information
 3229 and intelligence can be disseminated using LNOs or regularly scheduled logpacks.

3230 *Note.* When posting information to a website, the intended recipients must be notified when new
 3231 or critical information has been posted; simply posting information to a website does not ensure
 3232 that the intended user has received it.

- 3233 ● **Dissemination Procedures.** The G-2/S-2 and intelligence personnel at all levels assess the
 3234 dissemination of intelligence and intelligence products. Disseminating intelligence
 3235 simultaneously to multiple recipients is one of the most effective, efficient, and timely methods.
 3236 This can be accomplished through various means; for example, push, broadcast. However,
 3237 within the current tactical intelligence architecture, reports and other intelligence products move
 3238 along specific channels. The staff helps streamline information distribution within these
 3239 channels by ensuring dissemination of the right information in a timely manner to the right
 3240 person or element. There are three channels through which commanders and their staffs
 3241 communicate:
 - 3242 ■ **Command Channel.** The command channel is the direct chain-of-command link that
 3243 commanders, or authorized staff officers, use for command-related activities. Command
 3244 channels include command radio nets, video teleconferences, and the Maneuver Control
 3245 System.
 - 3246 ■ **Staff Channel.** The staff channel is the staff-to-staff link within and between headquarters.
 3247 The staff uses the staff channel for control-related activities. Through the staff channel, the
 3248 staff coordinates and transmits intelligence, controlling instructions, planning information,
 3249 and provides early warning information and other information to support C2. Examples of

FOR OFFICIAL USE ONLY

- 3250 staff channels include the operations and intelligence radio net, telephone, the staff huddle,
 3251 video teleconference, and the warfighting function-specific components of DCGS-A to
 3252 provide information and intelligence to the rest of the intelligence architecture.
- 3253 ■ **Technical Channels.** Staffs typically use technical channels to control specific activities.
 3254 These activities include fire direction and the technical support and SCI reporting channels
 3255 of intelligence and ISR operations. The SIGINT tasking and reporting radio net, intelligence
 3256 broadcast communications, and the wide area networks supporting single intelligence
 3257 discipline collection, processing, and production are examples of technical channels.
 - 3258 ● **Presentation Techniques and Procedures.** The staff’s objective in presenting information is to
 3259 provide the commander with relevant information. The presentation method is based on the
 3260 commander’s guidance. Table 4-1 lists the three general methods that the staff uses to present
 3261 information and meet its information objective. Specific techniques include METT-TC,
 3262 PMESII, and PMESII-PT. DCGS-A contains standard report formats, maps, and mapping tools
 3263 that assist the staff in presenting information in written, verbal, and graphic form. Audio and
 3264 video systems, such as large format displays and teleconferencing systems, enable the staff to
 3265 use a combination of the methods in multimedia presentations.

Table 4-1. Presentation methods and products

<i>Method</i>	<i>Products</i>
Written Narrative	Reports, Estimates, and Studies
Verbal Narrative	Briefings (information, decision, mission, and staff)
Graphic	Charts, Overlays, and Electronic Displays

3266 **Intelligence Communications Architecture**

3267 4-61. The intelligence communications architecture transmits intelligence and information to and from
 3268 various ISR elements, units, and agencies by means of automation and communication systems. The
 3269 DCGS-A enterprise is the primary method for providing intelligence products to users. With the continued
 3270 development of sensors, processors, and communications systems, it is increasingly important to
 3271 understand the requirements of establishing effective communications architecture. The G-2/S-2 must
 3272 identify the specific intelligence warfighting function requirements of the unit’s overall communications
 3273 architecture. Refer to FM 2-33.5 for more information on intelligence reach.

3274 4-62. The following are some (but not all) of the questions which the staff must answer in order to
 3275 establish the intelligence communications architecture:

- 3276 ● Where are the unit’s collectors?
- 3277 ● What and where are the unit’s processors?
- 3278 ● Where are the unit’s intelligence production elements?
- 3279 ● Where are the unit’s decision makers?
- 3280 ● How does the unit disseminate information from its producers to its decision makers and/or
 3281 consumers?
- 3282 ● Are the systems which the unit’s collectors, producers, processors, and consumers use
 3283 compatible with each other? If not, what is the plan to overcome this challenge?
- 3284 ● How can the unit access databases and information from higher and other agencies? Are there
 3285 special requirements necessary to access these databases such as security clearance, polygraph,
 3286 training, and certification?

FOR OFFICIAL USE ONLY

3287 ***Knowledge Management***

3288 4-63. Knowledge management is an important part of dissemination. The right information must flow to
3289 the right users at the right time without inundating the users with either extraneous or too much
3290 information. The G-2/S-2 must also ensure that users do not receive the same information from the same
3291 source multiple times. Circular reporting could result in erroneous analysis by intelligence personnel or
3292 unsubstantiated decisions by commanders.
3293

3294 ***Granting Access***

3295

3296 ***Sharing***

3297

3298 ***Posting***

3299

3300 ***Intelligence Reach***

3301 4-64. Intelligence reach is an important part of the intelligence effort. Intelligence reach allows intelligence
3302 analysts to retrieve existing information, intelligence products, and data which can support answering the
3303 CCIRs from outside the unit in a timely manner without having to wait for an answer to an RFI or an ISR
3304 task. The information, intelligence products, or data retrieved can then be evaluated for use in the unit's
3305 intelligence products or analysis.

3306 ***Updating the COP***

3307

3308 ***Commander's Input***

3309 4-65. Commander's input is provided at the commander's discretion. Commander's input is the key
3310 element in focusing the intelligence effort. This input directly influences the focus of the unit's ISR effort,
3311 the intelligence collection assets, and the intelligence analysis resources. It also determines which
3312 intelligence products are developed, as well as the format of the products.

3313

FOR OFFICIAL USE ONLY

3314

PART THREE

3315

Military Intelligence Disciplines

3316

Part Three provides a more detailed explanation of the intelligence disciplines introduced in Part One of this manual.

3317

3318

Chapter 5 defines and discusses the role and fundamentals of the All-source Intelligence discipline.

3319

3320

Chapter 6 defines and discusses the role and fundamentals of the Counterintelligence discipline.

3321

3322

Chapter 7 defines and discusses the role and fundamentals of the Human Intelligence discipline.

3323

3324

Chapter 8 discusses the Geospatial intelligence discipline and its role in Army operations.

3325

3326

Chapter 9 defines and discusses the role and fundamentals of the Imagery Intelligence discipline.

3327

3328

Chapter 10 defines and discusses the role and fundamentals of the Measurement and Signature Intelligence discipline.

3329

3330

Chapter 11 defines and discusses the role and fundamentals of the Open-Source Intelligence discipline.

3331

3332

Chapter 12 defines and discusses the role and fundamentals of the Signals Intelligence discipline.

3333

3334

Chapter 13 defines and discusses the role and fundamentals of the Technical Intelligence discipline.

3335

3336

Chapter 5

3337

All-Source Intelligence

3338

DEFINITION

3339

5-1. All-source intelligence is defined as the intelligence products, organizations, and activities that incorporate all sources of information and intelligence, including open-source information, in the production of intelligence. All-source intelligence is a separate intelligence discipline, as well as the name of the function used to produce intelligence from multiple intelligence or information sources.

3340

3341

3342

FOR OFFICIAL USE ONLY

3343 5-2. Army units plan and conduct operations based off the all-source intelligence assessment developed
3344 by the intelligence section. The all-source intelligence assessment is expressed as part of the intelligence
3345 running estimate.

3346 5-3. All-source intelligence operations are continuous and occur throughout the operations process and
3347 the intelligence process. Most of the products resulting from all-source intelligence are initially developed
3348 during planning and updated as needed during operations.

3349 **ROLE**

3350 5-4. The operational environment provides an ever-growing volume of data and information available
3351 from numerous sources, from which the commander can use to achieve situational understanding.
3352 Situational understanding enables the commander to—

- 3353 ● Make decisions in order to influence the outcome of the operation.
- 3354 ● Prioritize and allocate resources.
- 3355 ● Assess and take risks.
- 3356 ● Understand the needs of the higher and subordinate commanders.

3357 5-5. The commander depends upon a skilled G-2/S-2 working within the commander’s intent to provide
3358 sound IPB, support the commander’s ISR effort and provide all-source intelligence analysis, conclusions,
3359 and projections of future conditions or events.

3360 **FUNDAMENTALS**

3361 5-6. *Intelligence is the product resulting from collection, processing, integration, evaluation, analysis,*
3362 *and interpretation of available information concerning foreign nations, hostile, or potentially hostile forces*
3363 *or elements, or areas of actual or potential operations. This term is also applied to activity which results in*
3364 *the product and to the organizations engaged in such activity (JP 2-0). Using information from all*
3365 *available sources, all-source analysts conduct analysis and produce timely, relevant, accurate, predictive,*
3366 *and tailored intelligence that satisfies the commander’s requirements. All-source analysis provides an*
3367 *overall picture of the enemy, terrain and weather, and civil considerations. Thorough all-source analysis*
3368 *reduces the possibility of error, bias, and misinformation through the consideration of multiple sources of*
3369 *information and intelligence.*

3370 **PLANNING**

3371 5-7. During each step of the MDMP the intelligence staff is responsible for providing well-defined,
3372 specific all-source intelligence products and tools. These are the “deliverables” expected and required by
3373 the commander and staff during the planning process:

- 3374 ● Enemy threat characteristics.
- 3375 ● Enemy situation templates and COA statements.
- 3376 ● Event template and event matrix.
- 3377 ● HPT list (HPTL).
- 3378 ● Weather effects matrix.
- 3379 ● Modified combined obstacle overlay (MCOO) and terrain effects matrix.
- 3380 ● Civil Consideration (ASCOPE) IPB overlays.

3381 **MISSION ANALYSIS**

3382 5-8. A thorough mission analysis is crucial to planning. Both the process and products of mission analysis
3383 help commanders refine their situational understanding and determine their mission. Accurate situational
3384 understanding enables them to better visualize the operation. There are 17 separate tasks associated with

FOR OFFICIAL USE ONLY

3385 mission analysis that depend on all-source intelligence operations. Generally, the intelligence portion of
 3386 mission analysis is an evaluation of the following battlefield effects: threat, terrain, weather, and civil
 3387 considerations (ASCOPE). Additionally, it includes an analysis of the higher headquarters plan or order to
 3388 determine critical facts and assumptions; specified, implied, and essential tasks; and constraints that effect
 3389 ISR operations. Endstate is the development of an initial ISR plan, the refinement of the commander's
 3390 estimate based on a clear understanding of the situation, and the staff refining staff running estimates based
 3391 on that same understanding. To avoid misunderstanding and ensure there is a clear and common
 3392 understanding of what is fact and what is assumption at this point, the all-source analyst must tell the
 3393 commander and staff "what he knows and why he knows it, what he thinks and why he thinks it, what he
 3394 does not know and what he is doing about it". This promotes critical thinking and generates the staff
 3395 discussion required to formulate sound courses of action.

3396 5-9. Task 1: Analyze Higher Headquarters Order. The intelligence staff analyzes the higher headquarters'
 3397 order to determine how that commander and intelligence view the enemy. In order to provide the best
 3398 possible support to the commander and minimize the amount of time needed to complete products, the
 3399 intelligence staff conducts parallel and collaborative planning with the higher headquarters intelligence
 3400 staff as that staff completes its planning.

3401 5-10. Task 2: Perform Initial Intelligence Preparation of the Battlefield (IPB). The intelligence officer
 3402 leads the staff through the IBP process. The other staff sections assist the intelligence section in developing
 3403 the IBP products required for planning. IPB starts during mission analysis, is refined during the rest of the
 3404 MDMP, and continues during the preparation and execution of operations. It consists of four steps: define
 3405 the operational environment, describe environmental effects on operations, evaluate the threat, and
 3406 determine threat courses of action. The major results of initial IPB are terrain and geospatial products
 3407 developed as a result of examining the physical and human characteristics of the area of operations, enemy
 3408 situational overlays, enemy event templates and matrices, high value target lists, the identification of
 3409 intelligence gaps that the commander uses to establish initial information requirements, and an initial ISR
 3410 plan.

- 3411 • Evaluate Military aspects of the Terrain. Utilizing the topographic (TOPO) team, analysts
 3412 conduct a detailed terrain analysis of the area of operations focused on natural and man-made
 3413 features that may effect operations. Using the OAKOC model (Observation and Fields of Fire,
 3414 Avenues of Approach, Key Terrain, Obstacles, Cover & Concealment), the analyst briefs the
 3415 commander and staff on the effects the terrain may have on both friendly and enemy forces. The
 3416 analyst also briefs what effect the weather will have on terrain. The general product resulting
 3417 from terrain analysis is the Modified Combined Obstacle Overlay (MCOO). See FM 2-01.3 for a
 3418 detailed explanation of terrain analysis and the other standard products developed as a result of
 3419 it.
- 3420 • Evaluate Civil Considerations (ASCOPE) Analysis. ASCOPE is an acronym for area, structures,
 3421 capabilities, organizations, people, and events. These are the broad categories the Army uses to
 3422 analyze and describe the civil considerations that may have an effect on operations. Using the
 3423 ASCOPE model, the analyst briefs the commander and staff on the effects urban centers may
 3424 have on friendly and enemy forces. There is no standard product resulting from this analysis.
 3425 The G2/S-2 generally briefs a series of products developed based on the situation. See FM 2-
 3426 01.3 and FM 3-06 for a detailed explanation of ASCOPE analysis and the standard products
 3427 developed as a result of it.
- 3428 • Evaluate Weather Conditions and Effects. The USAF weather team assigned to the intelligence
 3429 section provides weather forecasting and analysis under the direction of the intelligence officer.
 3430 Using the Integrated Weather Effects Decision Aid (IWEDA) function in the Integrated
 3431 Meteorological System (IMETS) program, the intelligence section briefs the commander and
 3432 staff on the weather forecast and how it will affect warfighting functions in general as well as
 3433 personnel and equipment specifically. See FM 2-01.3 for a detailed explanation of weather
 3434 analysis.

FOR OFFICIAL USE ONLY

- 3435
- 3436
- 3437
- 3438
- 3439
- 3440
- 3441
- 3442
- 3443
- 3444
- 3445
- 3446
- 3447
- 3448
- 3449
- 3450
- 3451
- 3452
- 3453
- 3454
- 3455
- 3456
- 3457
- 3458
- 3459
- 3460
- 3461
- 3462
- 3463
- 3464
- 3465
- 3466
- 3467
- 3468
- 3469
- 3470
- 3471
- 3472
- 3473
- 3474
- 3475
- 3476
- 3477
- 3478
- 3479
- 3480
- 3481
- 3482
- 3483
- 3484
- 3485
- Develop Enemy threat characteristics. In order to accurately depict how an enemy commander will dispose and maneuver forces on the battlefield an analyst must understand how the enemy is organized and equipped, what the enemy's capabilities are, and how the enemy has employed forces in the past. An understanding of threat characteristics and detailed organizational charts assist in this analysis. This also helps identify what signatures the enemy gives off that can be collected by friendly ISR assets. Maintaining accurate threat characteristics is also essential in conducting combat assessment. This applies to regular and irregular forces as well as insurgent and terrorist organizations. Threat characteristics for conventional forces are generally available within the intelligence community. The analyst will generally have to develop threat characteristics for emerging threats like terrorists and insurgents. This is done by using information gained from national and theater intelligence organizations as well as from the publications of these types of threat groups.
 - Develop Enemy Situation Templates (ENSITEMP). Depending on the mission, there are three types of ENSITEMPs generally required for planning. The first two are used in conventional operations; showing the enemy conducting offensive and defensive operations against friendly forces. The third is used in unconventional operations; showing non-conventional forces conducting operations against friendly forces in complex terrain such as an urban area. Each of these overlays is a graphic depiction of the accompanying enemy COA statement. Together, they communicate the enemy's disposition, objectives, goals and endstate, main and shaping efforts, and how the enemy will maneuver. Additionally, these products graphically and textually explain the enemy's intent for fires, ISR, IO, and logistics. Finally, they explain the enemy's failure options and a recommendation on how to defeat the enemy. Both the overlay and statement are included in the mission analysis briefing. Depending on the mission, the analyst will generally develop more than one ENSITEMP to articulate other possible enemy COAs.
 - Identify High Value Target List (HVTL). Every ENSITEMP and ECOA statement is accompanied by an HVTL that describes and prioritizes in terms of their relative worth those assets that the enemy commander requires for to achieve stated objectives. The analyst develops the HVTL in coordination with the rest of the staff.
 - Develop an Event Template and Matrix. Developed as the basis for the decision support template (DST) and the ISR overlay, this tool assists in the identification of the commander's decision points and in determining ISR strategies. It ensures a consistent and well reasoned portrayal of enemy capabilities throughout the planning process. It is critical in tying ISR and maneuver together as well as assisting in the development of a plan that allows the commander to get inside the enemy's decision cycle. The event template and matrix are not briefed during mission analysis but they must be ready for COA development.
- 5-11. Task 3: Determine Specified, Implied, and Essential Tasks. The analyst analyzes the higher headquarters order to identify the specified ISR tasks that have been assigned to the unit and develop any implied tasks that must be performed to accomplish stated specified tasks. The analyst then provides a list of specified and implied tasks to the operations section and assists in determining essential tasks for inclusion in the unit's mission statement.
- 5-12. Task 4: Review Available Assets. The analyst reviews the status of the unit's ISR assets, any additions or deletions made by the higher headquarters order, and what higher echelon support is available for the operation. From this analysis, the analyst then determines if the unit has the assets it needs to accomplish all collection tasks. If there are shortages, the intelligence section identifies them and makes recommendations for additional resources.
- 5-13. Task 5: Determine Constraints. A higher commander normally places some constraints on subordinate commanders. Constraints are restrictions placed on the command by a higher command. They dictate an action or inaction, thus restricting the freedom of action a subordinate commander has for planning. A typical constraint for ISR operations is establishing a limit of advance for air or ground reconnaissance. Constraints are normally contained in the scheme of maneuver, paragraph, concept of

FOR OFFICIAL USE ONLY

3486 operations paragraph, or coordinating instructions paragraph in the base order. However, they are
3487 sometimes stated in the annexes to the order as well.

3488 5-14. Task 6: Identify Critical Facts and Assumptions. Along with the rest of the staff members, the
3489 intelligence analyst is responsible for gathering two categories of information concerning assigned tasks;
3490 facts and assumptions.

3491 5-15. Task 7: Perform Risk Assessment. This task is performed by the operations section with assistance
3492 from the rest of the staff. See FM 5.0 and FM 100-14 for an explanation of risk assessment.

3493 5-16. Task 8: Determine Initial Commander's Critical information Requirements (CCIR) and Essential
3494 Elements of Friendly Information (EEFI). Determine initial information requirements. This is the first step
3495 in developing a collection plan. PIR are not developed by the staff until COA analysis and are not
3496 approved by the commander until COA approval. In the mission analysis briefing, after stating "what he
3497 knows, what he thinks he knows, and what he does not know" the analyst recommends what information
3498 the intelligence section should be collecting and analyzing in support of continued planning and COA
3499 development. Identifying information requirements at this time helps the commander filter information
3500 available by defining what is important to mission accomplishment. It also helps to focus the efforts of the
3501 rest of the staff and subordinate commands.

3502 5-17. Task 9: Determine the Initial ISR Plan. The operations section is the staff proponent of the ISR plan.
3503 It is an integrated staff product executed by the unit at the direction of the commander. The operations
3504 officer, assisted by the intelligence section, uses the ISR plan to task and direct available ISR assets to
3505 answer CCIR (PIR and FFIR) and other intelligence requirements. The intelligence section must have its
3506 input and products ready to be published as part of the Warning Order that the S-3 issues at the conclusion
3507 of mission analysis.

3508 5-18. Task 10: Update the Operational Timeline. Using the enemy operational timeline developed during
3509 IPB and illustrated by the event template and matrix, the commander and staff compare the operational
3510 timeline established by the higher headquarters order to determine windows of opportunity to exploit
3511 enemy vulnerability or times when the unit may be at risk from enemy activity.

3512 5-19. Task 11: Write the Restated Mission. The unit chief of staff or executive officer normally drafts a
3513 recommended mission statement based on the staff's mission analysis and presents it for approval to the
3514 commander at the conclusion of the mission analysis briefing. The intelligence section has already
3515 provided input for the restated mission during task three and normally has no further input at this time.

3516 5-20. Task 12: Deliver a Mission Analysis Briefing. Time permitting, the staff briefs the commander on its
3517 mission analysis using the outline provided in FM 5.0. The intelligence analyst is responsible for briefing
3518 the initial IBP products developed for threat, terrain, weather, and civil considerations (ASCOPE). The
3519 analyst may also brief the initial ISR plan if the unit is in a position to begin collection operations. The
3520 mission analysis briefing is a decision briefing that results in an approved restated mission, commander's
3521 intent, and commander's planning guidance. The analyst, presents only that relevant information the
3522 commander needs to develop situational understanding and formulate planning guidance.

3523 5-21. Task 13: Approve the Restated Mission. Immediately after the mission analysis briefing the
3524 commander approves a restated mission. Once approved, the restated mission becomes the unit mission.
3525 The analyst has no role in this task.

3526 5-22. Task 14: Develop the Initial Commander's Intent. The intelligence section is generally concerned
3527 with commander's intent as it applies to all warfighting functions. However, as the staff proponent, the
3528 intelligence analyst is most concerned with the intelligence warfighting function and what the
3529 commander's intent is for ISR. Given that, the analyst advises the commander on commander's intent for
3530 ISR. The analyst makes that recommendation informally prior to the mission analysis briefing or at the
3531 conclusion of the intelligence portion of the briefing. The commander considers this recommendation prior
3532 to formulating his intent.

FOR OFFICIAL USE ONLY

3533 5-23. Task 15: Issue the Commander's Planning Guidance. The commander issues his planning guidance
3534 after the mission analysis briefing and before the start of course of action development. The analyst has no
3535 role in this task unless asked for additional input from the commander.

3536 5-24. Task 16. Issue a Warning Order. Immediately after the commander gives planning guidance the
3537 operations officer issues a warning order. At a minimum, the intelligence section input into this order is the
3538 enemy situation paragraph, priority of intelligence collection, priority of intelligence support, intelligence
3539 tasks to subordinate units, and PIR. Additionally, if initial IPB products have not yet been made available
3540 to higher headquarters and subordinate commands they should be issued with the warning order.

3541 5-25. Task 17. During the rest of the MDMP, the commander and staff periodically review all facts and
3542 assumptions. New facts may alter requirements and require a re-analysis of the mission. Assumptions may
3543 have become facts or may have even become invalid. Whenever the facts or assumptions change, the
3544 commander and staff assess the impact of these changes on the plan and make the necessary adjustments,
3545 including changing the CCIR, if necessary.

3546 **COURSE OF ACTION (COA) DEVELOPMENT**

3547 5-26. . The purpose of COA development is to update staff running estimates and prepare COA options for
3548 the commanders consideration.. The staff develops friendly COAs based on facts and assumptions
3549 identified during IPB and mission analysis. Incorporating the results of IPB into COA development ensures
3550 that each friendly COA takes advantage of the opportunities the environment and threat situation offer. The
3551 intelligence analyst works closely with the operations section and the rest of the staff to analyze relative
3552 combat power and develop friendly COAs that can defeat enemy operations. All friendly COAs are
3553 developed off the enemy situation template and enemy event template/matrix the analyst produced during
3554 mission analysis. At the conclusion of COA development the intelligence section has completed draft
3555 information requirements for each friendly COA as well as a draft ISR overlay and synchronization matrix
3556 in preparation for COA analysis.

3557 **COA ANALYSIS (WARGAMING)**

3558 5-27. . COA Analysis is a disciplined process that includes rules and steps followed in sequence. It relies
3559 heavily on an understanding of doctrine, tactical judgment, and experience. Each staff member
3560 participating must come prepared with the full knowledgeable of the warfighting function represented. The
3561 intelligence analyst has two areas of responsibility in the wargame; role-play the enemy commander and
3562 act as the ISR officer. First, as the enemy commander, using the enemy situation template as a start-point
3563 and the event template/matrix as a guide, the analyst develops critical enemy decision points in relation to
3564 friendly COAs, projects enemy reactions to friendly actions, and projects enemy losses. Second, as the ISR
3565 officer, the analyst identifies new information requirements, assists the staff in developing PIR, refines the
3566 situation and event templates, develops the ISR overlay and synchronization matrix, and assists in the
3567 development of the High payoff targets and the decision support template (DST). At the conclusion of the
3568 wargame, pending COA approval by the commander, every intelligence product that must be published
3569 with the order is complete.

3570 **COA APPROVAL**

3571 5-28. . At the conclusion of the wargame the staff identifies its preferred COA and makes a
3572 recommendation to the commander. This is the COA decision briefing. During this briefing the analyst will
3573 brief any changes to the current enemy situation and any environmental factors that have changed since the
3574 commander was last briefed.

3575 **ORDERS PRODUCTION**

3576 5-29. . The staff led by the operations prepares the order by turning the selected COA into a clear, concise
3577 concept of operations and supporting information. The order provides all the information subordinate

FOR OFFICIAL USE ONLY

3578 commands need to plan and execute their operations. However, this is not the first time subordinate
3579 commanders and their intelligence staffs have seen this data. As stated previously, within the parallel and
3580 collaborative planning process, intelligence analysts at all echelons have been involved in the orders
3581 process; reviewing each other's intelligence products as they were developed and, at this point, are
3582 clarifying changes and submitting requests for additional information and product support. Prior to the
3583 order being issued the intelligence section will conduct an orders crosswalk with the rest of the staff as
3584 directed by the brigade operations officer.

3585 **RUNNING ESTIMATE, INTELLIGENCE RUNNING ESTIMATE AND THE COP**

3586 5-30. A running estimate is a staff section's continuous assessment of current and future operations to
3587 determine if the current operation is proceeding according to the commander's intent and if future
3588 operations are supportable. (FM 3-0) Running estimates provide information, conclusions, and
3589 recommendations from the perspective of each staff section. They serve as a staff technique to support the
3590 commander's visualization and decision making, as well as the staff's tool for assessing during preparation
3591 and execution. In the running estimate, staff officers continuously update their conclusions and
3592 recommendations as they evaluate the impact of new facts.

3593 5-31. Each staff section produces a running estimate. The main difference between the running estimate
3594 and the old staff estimates is the emphasis on not only continuously updating the facts of the estimate but
3595 also continuously updating the conclusions and recommendations while including projections of future
3596 conditions of the entire AO.

3597 5-32. Current doctrine emphasizes the COP as the primary tool that provides the commander a
3598 visualization of the current situation. All staff sections provide their respective input to the COP.

3599 5-33. The portion of the COP that depicts the threat situation is currently limited to displaying the
3600 locations and dispositions of threat forces in a relatively static manner, sometimes referred to as snapshots
3601 in time. The threat situation portion of the COP requires analysis to provide the required level of detail.
3602 DCGS-A will be the means for integrating this information into the COP.

3603 5-34. While the COP is primarily a display of current intelligence and information, the running estimate
3604 requires the merging of the staff's cognitive processes with automation applications. The primary focus of
3605 the staff's cognitive process is to present predictive or anticipatory intelligence in support of the
3606 commander's decision making or situational understanding. The running estimate integrates the running
3607 estimates from each staff section. The intelligence staff's input to the running estimate is the intelligence
3608 running estimate. Training is required (not just within MI) in order to successfully build and maintain the
3609 staff's running estimate and COP integration.

3610 5-35. The intelligence running estimate is a continuous flow and presentation of relevant information and
3611 predictive intelligence that, when combined with the other staff running estimates, enables the
3612 commander's visualization and situational understanding of the AOI in order to achieve information
3613 superiority. The intelligence running estimate requires constant verification to support situational
3614 understanding of the current situation as well as predictive assessments for future operations.

3615 5-36. The intelligence staff's running estimate details the ability of the intelligence staff to support
3616 operations. It focuses analysis and detects potential effects on operations. It supports the commander's
3617 visualization throughout the operation. The intelligence running estimate provides a fluid and current
3618 picture based on current intelligence products and reports and predictive estimates of future threat activity.
3619 The intelligence running estimate consists of all of the continuously updated and monitored intelligence
3620 that is available but that is then filtered to provide the specific intelligence relevant to current and projected
3621 future operations.

3622 5-37. The intelligence running estimate is initially developed after the generating knowledge step of the
3623 intelligence process. The intelligence running estimate is then refined and improved following mission
3624 analysis. It is further refined and improved based on the results of ISR operations. It is updated as required

FOR OFFICIAL USE ONLY

3625 upon changes in the enemy situation, terrain, weather and civil considerations. The intelligence running
3626 estimate includes—

- 3627 ● Mission
- 3628 ● Area of Operations
- 3629 ● Enemy/Threat situation
- 3630 ● Enemy/Threat capabilities
- 3631 ● Conclusions

3632 5-38. The G-2/S-2 must clearly understand the weather and terrain effects and the G-2/S-2 must be able to
3633 visualize the AO before producing the intelligence staff's running estimate. This understanding facilitates
3634 accurate assessments and projections regarding the threat; the threat situation (including strengths and
3635 weaknesses); threat capabilities and an analysis of those capabilities (COAs available to the threat); and
3636 conclusions drawn from that analysis. The estimate details threat characteristics into threat capabilities and
3637 projections of future threat actions.

3638 OPERATIONS

3639 5-39. Successful ISR operations depend of timely, relevant, and well-reasoned all-source analysis.
3640 Successful ISR operations are not based on advanced technology or intelligence reach. By themselves, the
3641 Army's array of collection systems, intelligence processors, and network advantages will not ensure the
3642 commander's information requirements are satisfied. These are just tools that, if used correctly, can
3643 enhance a unit's ability to answer questions in a timely manner.

3644 5-40. The key to successful ISR operations is an ISR plan that:

- 3645 ● *Is developed from well-reasoned enemy situation overlays, course of action statements, and*
3646 *event templates/matrices.*
- 3647 ● Is driven by the commander's CCIR and is focused on command directed tasks.
- 3648 ● Is tied to the commander's decisions (decision points) or actions (lines of operation).
- 3649 ● Facilitates the commander's visualization of his area of operations.
- 3650 ● Is prepared jointly by the intelligence section, and the rest of the staff.
- 3651 ● Remains synchronized with the scheme of maneuver.
- 3652 ● Is issued and updated as part of the orders process.
- 3653 ● Assigns appropriate collection tasks to subordinate units.
- 3654 ● Requests intelligence support as needed from higher and adjacent units.

3655 5-41. Develop Requirements (Requirements Management). Requirements management is the responsibility
3656 of the all-source analysis / fusion section. Requirements management is the process of identifying,
3657 prioritizing, and refining gaps in data, relevant information, and knowledge concerning the operational
3658 environment that must be resolved in order for the commander to achieve situational understanding.
3659 Requirements are developed prior to conducting an operation and during on-going operations. An
3660 important element in developing requirements is constant collaboration between all warfighting functions
3661 as well as between the analysis and collection management cells to redefine information requirements and
3662 focus the ISR effort as the situation develops.

3663 5-42. While the rest of the staff contributes to this effort, the analysis cell is the primary element
3664 responsible for developing requirements during planning and steady-state operations. Using the
3665 commander's current stated requirements, the brigade mission statement, input from the brigade staff, and
3666 input from higher headquarters the analysis cell identifies intelligence gaps and forwards them to the
3667 intelligence officer and operations officer for consideration as PIR and collection requirements. Because
3668 the ISR synchronization process is continuous and non-sequential, requirements are developed throughout
3669 the process and at all stages or phases of operational planning, preparation, and execution.

FOR OFFICIAL USE ONLY

3670
3671
3672
3673
3674
3675
3676
3677

5-43. The endstate of requirements development is to produce new intelligence requirements that are developed from ongoing operations that will drive new operations, branches and sequels. Effective requirements management depends on detailed IPB; including the maintenance of the intelligence running estimate, to include enemy situation templates/course of action statements as well as the development of event templates/matrices. Timely development of an event template/matrix IAW the unit battle rhythm is critical to the development of the decision support template, intelligence synchronization matrix, ISR overlay, and the execution of ISR operations.

FINAL DRAFT

FOR OFFICIAL USE ONLY

3678

Chapter 6

3679

Counterintelligence

3680 DEFINITION

3681 6-1. Counterintelligence counters or neutralizes intelligence collection efforts through collection, CI
3682 investigations, operations, analysis and production, and technical services and support. CI includes all
3683 actions taken to detect, identify, exploit, and neutralize the multidiscipline intelligence activities of friends,
3684 competitors, opponents, adversaries, and enemies. It is the key intelligence community contributor to
3685 protect US interests and equities. It assists in identifying essential elements of friendly information
3686 (EEFIs), identifying vulnerabilities to threat collection, and actions taken to counter collection and
3687 operations against US forces. Refer to FM 2-22.2 for details concerning CI mission and functions.

3688 MISSION

3689 6-2. The mission of Army CI is to conduct aggressive, comprehensive, and coordinated investigations,
3690 operations, collection, analysis and production, and technical services. These functions are conducted
3691 worldwide to detect, identify, assess, counter, exploit, or neutralize the AFIST collection threat to the US
3692 Army and DOD, in order to protect the lives, property, or security of Army forces. Army CI has four
3693 primary mission areas: counterespionage; support to FP; support to research and technology protection;
3694 cyber CI.

3695 ROLE

3696 6-3. The role of CI is to deny, degrade, disrupt, or mitigate AFIST ability and capability to successfully
3697 execute intelligence collection targeting US or friendly force interests. CI will focus on countering AFIST
3698 intelligence collection activities targeting information or material concerning US or friendly force
3699 personnel, activities, operations, plans, equipment, facilities, publications, technology, or
3700 documents—either classified or unclassified. It does this without official consent of designated US release
3701 authorities, for any purpose that could cause damage or otherwise adversely impact the interests of national
3702 security of the US ability to fulfill national policy and objectives.

3703 6-4. CI elements are instrumental in contributing to situational awareness in the area of influence. CI
3704 elements may corroborate other intelligence discipline information as well as cue other intelligence assets
3705 through the CI core competencies and through CI technical services.

- 3706 ● CI core competencies are investigations of national security crimes within CI jurisdiction,
3707 collection of AFIST threat information and targeting, operations, and analysis and production.
- 3708 ● CI technical services include computer network operations (CNO), technical surveillance
3709 countermeasures (TSCM), and polygraph. CI focuses on combating AFIST intelligence
3710 activities targeting Army personnel, plans, operations, activities, technologies, and other critical
3711 information and infrastructure.
- 3712 ● With proper approval, CI may employ electronic surveillance, investigative photography, cyber
3713 CI support, polygraph, and TSCM.

FOR OFFICIAL USE ONLY

3714 COUNTERINTELLIGENCE FUNCTIONS

3715 6-5. CI functions are interrelated, mutually supporting, and can be derived from one another. No single
 3716 function or technical capability can defeat AFIST intelligence efforts to target US interests. CI functions
 3717 are discussed below.

3718 CI INVESTIGATIONS

3719 6-6. Investigative activity is essential to countering the adversary intelligence threat to Army interests. CI
 3720 places emphasis on investigative activity to support force, infrastructure and technology protection,
 3721 homeland defense, information assurance, and security programs. CI investigations focus on resolving
 3722 allegations of known or suspected acts that may constitute National Security Crimes under US law which
 3723 include—

- 3724 ● Treason.
- 3725 ● Espionage.
- 3726 ● Subversion.
- 3727 ● Sedition.

3728 6-7. Other CI investigations include unreported contact with foreign government personnel, persons or
 3729 groups involved in foreign terrorism or intelligence, or unauthorized requests for classified or sensitive
 3730 unclassified information, and military personnel or Army civilians who perform unofficial travel to those
 3731 countries designated in the operational planning list.

3732 6-8. The primary objective in any CI investigation is the detection, identification, exploitation, and/or
 3733 neutralization of adversary intelligence threats directed against the US Army. CI investigations are also
 3734 conducted to identify systemic security problems that may have damaging repercussions to Army
 3735 operations and national security interests. All CI investigations are conducted within guidelines established
 3736 in
 3737 AR 381-10, AR 381-12, AR 381-20, applicable DOD policy and directives, and US laws.

3738 CI OPERATIONS

3739 6-9. CI operations are characterized as those activities that are not solely associated with investigative,
 3740 collection, analysis, or production functions. CI operations can be either offensive or defensive in nature;
 3741 they are derived from or transition to a collection or investigative activity depending on the scope,
 3742 objective, or continued possibility for operational exploitation. CI operations fall into the following two
 3743 categories:

- 3744 ● **CI Support Operations.** These are defensive operations used to support Army operations,
 3745 technology protection, security projects, and programs. They include technical services support,
 3746 support to acquisition, FP, SAPs, international security, foreign visitor or contact, treaty
 3747 verification, information assurance, homeland defense, and advice and assistance programs
 3748 conducted by CI teams to improve the security posture of supported organizations. CI support
 3749 operations also include—
 - 3750 ■ Conducting inspections, security planning, and resolution of security problems.
 - 3751 ■ Developing classification guides.
 - 3752 ■ Conducting surveys.
 - 3753 ■ Conducting technical inspections.
 - 3754 ■ Providing pre-construction technical assistance.
 - 3755 ■ Conducting SAEDA briefings and other approved projects and programs.
- 3756 ● **CI Sensitive Operations.** These operations are generally offensive in nature and involve direct
 3757 or indirect operations against a known or suspected AFIST intelligence threat. These operations
 3758 include counterespionage and CI projects and are conducted by designated units.

FOR OFFICIAL USE ONLY

3759 **CI COLLECTION**

3760 6-10. **CI Collection Activities.** While CI and HUMINT both have a collection mission, it should be
 3761 understood that there are distinct differences between CI and HUMINT collection objectives. HUMINT
 3762 focuses on answering the CCIRs concerning the plans, intentions, capabilities, and disposition of the
 3763 adversary as a whole. CI specifically targets the AFIST intelligence collection threat targeting US forces.
 3764 CI collection is—

- 3765 ● The systematic acquisition of information concerning the AFIST intelligence collection threat
 3766 targeting US Army equities. CI elements conduct collection activities in support of the overall
 3767 CI mission.
- 3768 ● Conducted through the use of sources, elicitation, official liaison contacts, debriefings,
 3769 screenings, and OSINT to obtain information that answers the standing CI collection
 3770 requirements or other collection requirements based upon the CCIRs.
- 3771 ● Conducted to understand how AFIST is targeting US forces so other CI initiatives can be
 3772 devised to deny the adversary the ability to collect on, target, or react to US military operations.

3773 6-11. **CI Source Operations.** CI conducts source operations to gather information the commander needs
 3774 to make decisions in support of the overall mission. The commander focuses the CI effort by carefully
 3775 assigning missions and clearly defining the desired results. While using CI collection as a means of
 3776 targeting, the use of single-source reporting could lead to targeting based on tribal, regional, or cultural
 3777 differences rather than threat-based targeting. In all instances, CI reporting should be corroborated by other
 3778 sources of information and/or intelligence disciplines to determine accuracy and truthfulness prior to
 3779 targeting by the commander. CI source operations—

- 3780 ● Are not intended to be used as a substitute for tactical HUMINT military source operations
 3781 (MSO).
- 3782 ● Can be used to initiate CI investigations, identify potential leads for offensive operations, or
 3783 develop additional CI leads.
- 3784 ● Consist of three different collection categories:
 - 3785 ■ Offensive CI Operations (OFCO) activities support Army, Theater, Army component
 3786 commands (ACCs), Army service component commands (ASCCs), and local intelligence
 3787 requirements, as well as DOD, Joint Chiefs of Staff, unified and specified commands, JTF,
 3788 and multinational and national intelligence community strategic requirements in order to
 3789 deter, detect, and neutralize espionage. (For more information on OFCO, refer to
 3790 AR 381-47 (S)).
 - 3791 ■ CI Defensive Source Operations (DSO) are only employed by units with a CI investigative
 3792 and operational mission. CI DSO will not be employed in combat operations. CI DSO
 3793 activities are only employed by units with a CI investigative and operational mission. They
 3794 are conducted in support of theater-level operations in mature and stable environments to
 3795 answer theater-level information requirements. CI DSO will be proposed through the
 3796 submission of a CI Special Operation Concept and have to be approved by Commander,
 3797 INSCOM, or designated representative. (For more information concerning DSO, refer to
 3798 TC 2-22.201 (S)).
 - 3799 ■ CI Force Protection Source Operations (CFSO) use source operations to collect FP and
 3800 AFIST collection and threat I&W. CFSO are conducted in all OCONUS locations to satisfy
 3801 the supported commander's information requirements. CFSO is employed on the basis of a
 3802 CFSO OPLAN approved by the supported commander or the S/G/J/C2X if approval
 3803 authority has been delegated by the ASCC or JTF commander. CFSO will only be
 3804 conducted OCONUS except for unit training.

3805 6-12. **Liaison.** CI elements conduct liaison with US, multinational, and HN military and civilian agencies,
 3806 to include NGOs, for the purpose of obtaining information of CI interest and coordinating or deconflicting

FOR OFFICIAL USE ONLY

3807 CI activities. Liaison activities are designed to ensure a cooperative operating environment for CI elements
3808 and to develop CI leads for further exploitation.

3809 6-13. **Screening.** CI Screening is a systematic process for obtaining information of CI interest from a
3810 specific person or target audience. Information of CI interest includes all standing CI collection
3811 requirements established in AR 381-20, CCIRs, or any information that includes but is not limited to the
3812 plans, intentions, capabilities, methods of operation, personalities, structure, and personal associations with
3813 any AFIST entity.

3814 6-14. CI screening uses a variety of questioning techniques to obtain information. This includes
3815 interviewing methods using basic interrogatives to identify and exploit information of CI interest; a
3816 structured debriefing format utilizing a prepared question list when the source has knowledge of a specific
3817 topical interest; and elicitation utilizing a discreet form of questioning which does not let the source know
3818 the specific AOI of the CI Special Agent.

3819 *Note.* CI screening does not use any types of interrogation or screening approaches utilized by
3820 HUMINT collectors defined in FM 2-22.3. CI screening normally is not confrontational unless
3821 the source initiates a hostile attitude and forces the CI Special Agent to maintain control through
3822 the exercise of the CI Special Agent's official authority.

3823 6-15. Each of the interviewing methods can be used or combined dependent upon the situation. CI
3824 screenings include the following:

- 3825 ● **Local Employee Screening.** Local employee screening is conducted primarily to identify
3826 individuals who may be a security risk. It can, however, be used as a means to obtain
3827 intelligence information or to identify personnel with placement and access to be used for source
3828 operations.
- 3829 ● **CI Support to Joint Interrogation and Debriefing Centers.** During combat and other
3830 contingency operations, CI will normally be included in the manning and support requirements
3831 for Joint Interrogation and Debriefing Center (JIDC) operations. While the priority for
3832 intelligence collection during JIDC operations is focused on CCIRs and other HUMINT-specific
3833 collection requirements, JIDC operations offer an excellent opportunity for CI collection.
3834 Detainees held in JIDC facilities will include adversarial military, security, intelligence,
3835 insurgent, and terrorist personnel who can answer specific CI requirements to include but not
3836 limited to the plans, intentions, capabilities, methods of operation, personalities, structure, and
3837 personal associations of AFIST elements targeting US forces.
- 3838 ● **Local Community or Area Screening.** Local area screening is normally done in coordination
3839 with other operations such as a cordon and search operation. CI Special Agents accompany the
3840 forces conducting the operation and screen the general population to identify individuals of CI
3841 interest.

3842 6-16. **CI Debriefing.** CI debriefings focus on two different types of targets. Debriefing of repatriated US
3843 personnel or special category absentees and personnel who are pre-briefed and debriefed as part of an
3844 approved CI operation or project. CI personnel assigned to combat units may also participate in
3845 intelligence debriefing of US or multinational patrols or other tactical elements that may support the
3846 CCIRs. (For more information on CI debriefings, see FM 2-22.2.)

3847 6-17. **CI Technical Services and Support.** CI technical services are used to assist the CI functions of
3848 investigations, collections, and operations or to provide specialized technical support to a program or
3849 activity. The proliferation of sophisticated collection technology, surveillance, and eaves-dropping devices
3850 available in the commercial markets enables any AFIST the ability to increase their capability and
3851 effectiveness in collecting on US Army interests. To mitigate this increasing threat requires a specialized
3852 expertise. CI organizations with technically trained CI Special Agents are chartered with providing this

FOR OFFICIAL USE ONLY

3853 unique technical capability to augment and provide specialized support to the CI mission. This includes CI
3854 Special Agents trained to—

- 3855 ● Conduct physical and electronic surveillance in support of authorized CI investigative activities.
- 3856 ● Perform TSCM to identify adversarial electronic collection activities.
- 3857 ● Perform cyber CI activities that provide protection to information networks as well as to identify
3858 vulnerabilities and attempted intrusions into Army and DOD computer networks.
- 3859 ● Perform CI scope polygraph examinations in support of CI investigative activities and sensitive
3860 program support.

3861 **6-18. CI Covering Agent Program (CICAP).** CICAP is the assignment of a primary supporting CI
3862 Special Agent to a command or agency. This agent conducts all routine liaisons and provides advice and
3863 assistance to the unit. The agent must become fully knowledgeable with the unit's operations, security,
3864 personnel, and vulnerabilities. The agent is the point of contact for reporting information of actual or
3865 potential CI interest.

3866 ANALYSIS

3867 6-19. CI analysis is conducted as a single-source feed into the all-source intelligence analysis process and
3868 to focus CI operations. CI analysis and production will be accomplished at any level at which Army CI
3869 assets are assigned. CI analysis focuses on the plans, intentions, and capabilities of an AFIST entity known
3870 or suspected of targeting US forces for targeting and/or information exploitation to support FP of US
3871 personnel, property and operations; protect the R&D of critical technologies; and to support information
3872 operations to protect US forces information systems.

3873 Intelligence Analysis

3874 6-20. CI analysis should be focused on predictive, assessments of AFIST plans, intentions, and
3875 capabilities. CI analysis supports the development of countermeasures recommendations to deny, disrupt,
3876 or negate the ability of an AFIST entity to successfully collect and exploit information concerning US
3877 forces. Accurate CI analysis also increases the visibility of proactive and effective CI support and
3878 establishes credibility with the supported commander. This in turn leads commanders to trust and rely upon
3879 their CI assets and often give them more flexibility to execute CI operations.

3880 Operational Analysis

3881 6-21. Operational analysis allows the operational management elements (2X, Counterintelligence
3882 Coordinating Authority [CICA] and Operational Management Team [OMT] leaders) to gauge the
3883 effectiveness and success of their subordinate operational CI teams. Operational analysis—

- 3884 ● Is done through assessments on source production (quantity and quality), source vetting
3885 (reliability, accuracy, response to control), and requirements coverage.
- 3886 ● Also allows operational managers to deconflict CI operations and to provide direction and focus
3887 to eliminate redundancy and/or increase the efficiency of the CI teams.

3888 PRODUCTION

3889 6-22. CI products consist of but are not limited to target nomination, threat assessments, CI estimates, and
3890 investigative and intelligence information reports. CI is responsible for providing the AFIST threat
3891 assessment, which can stand alone or be included as part of a vulnerability assessment. Threat assessments
3892 are a comprehensive assessment of the plans, intentions, capabilities, tactics, and focus of a known or
3893 suspected AFIST entity. A vulnerability assessment is a detailed assessment of a unit, agency, facility,
3894 operation, or mission to identify vulnerabilities to security or operational TTP that could impact the
3895 successful execution of the mission or operation.

FOR OFFICIAL USE ONLY

3896 6-23. Vulnerability assessments are planned and coordinated by the unit FP officer and consists of multiple
 3897 agencies providing subject matter expertise to the final product which should include not just the
 3898 vulnerabilities but risk mitigation measures. (VAs are conducted to identify weaknesses and vulnerabilities
 3899 in security and FP posture and to provide countermeasures recommendations.) Finalized intelligence
 3900 derived from CI activities are incorporated into joint and national intelligence databases, assessments, and
 3901 analysis products. CI products are also incorporated into the COP to support battlefield situational
 3902 awareness. CI production takes place at all levels.

- 3903 ● Operational and tactical production includes—
 - 3904 ■ Spot reports and current intelligence.
 - 3905 ■ CI threat and/or vulnerability assessments tailored to specific activities, units, installations,
3906 programs, or geographic areas.
 - 3907 ■ CI studies to support contingency planning and major exercises.
 - 3908 ■ Studies of adversary intelligence organization, modus operandi, personnel, activities, and
3909 intentions that pose a current or potential threat to the supported command.
- 3910 ● Strategic products include—
 - 3911 ■ Assessments supporting national and Army programs including SAPs and acquisition
3912 programs.
 - 3913 ■ Worldwide assessments of the organization, location, funding, training, operations
3914 capabilities, and intentions of terrorist organizations.
 - 3915 ■ Global trends in adversary intelligence modus operandi.
 - 3916 ■ After-action studies of individual espionage cases.
 - 3917 ■ Analyses of the intelligence collection capabilities of international narcotics trafficking
3918 organizations.
 - 3919 ■ Multimedia threat products to support Army CI awareness programs.

3920 COUNTERINTELLIGENCE STRUCTURE

3921 6-24. CI organizations and force structure are designed to support the modular force construct through
 3922 scalable team, operations management, and technical channels packages. CI elements assigned to division,
 3923 battlefield surveillance brigades, ASCC, and strategic units are capable of operating at all echelons and
 3924 throughout the full spectrum of military operations. The Joint *2X organizational and operational concept
 3925 has been established in Army Force structure to decentralize CI operational approval and execution. As the
 3926 primary force provider for the DOD CI in contingency and combat operations, the establishment of the
 3927 *2X and the CICA throughout the Army ensures a trained and experienced cadre of CI professionals
 3928 capable of filling Army, joint, and combined 2X and CICA/Task Force Counterintelligence Coordinating
 3929 Authority (TFCICA) positions.

3930 ***2X**

3931 *Note.* *2X denotes the 2X staff officer at all echelons, S-2X (Brigade), G-2X (Division, Corps,
 3932 ASCC), J-2X (JTF), C-2X (Combined Task Force), and Army G-2X (Department of the Army
 3933 [DA] level).

3934 6-25. The *2X is the CI and HUMINT manager who is authorized to coordinate, deconflict, and
 3935 synchronize all CI and HUMINT missions in the area of intelligence responsibility. The *2X manages CI
 3936 and HUMINT intelligence requirements including HUMINT collection requirements, time-sensitive
 3937 collection requirements, report evaluations with source-directed requirements, and source assessments. At
 3938 each echelon the *2X Section may be structured differently, but there is always a requirement for three
 3939 components: CICA, a HUMINT operations cell (HOC), and an operations support cell (OSC). Figure 6-1
 3940 shows the 2X organization. The *2X is responsible for—

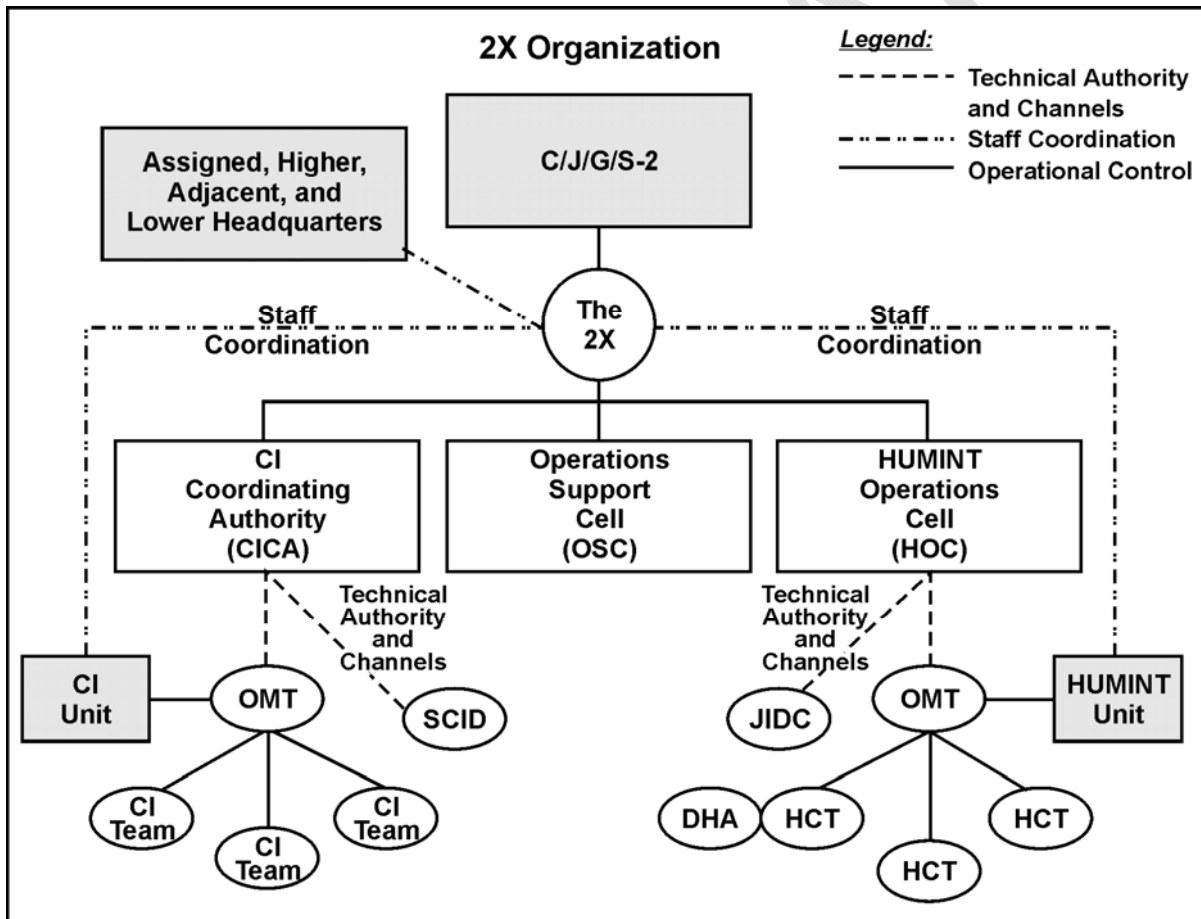
FOR OFFICIAL USE ONLY

3941
3942
3943
3944
3945
3946
3947
3948
3949
3950

- Participating in predeployment or deployment planning for CI and HUMINT assets in support of operations.
- Coordinating, through the HOC and TFCICA/CICA, all CI and HUMINT activities to support intelligence collection and the intelligence aspects of FP for the deployed commander.
- Managing collection requirements for CI and HUMINT in coordination with the requirements manager.
- Coordinating and deconflicting all CI and HUMINT operations within the operational area.
- Serving as the release authority for CI and HUMINT reporting.
- Releasing reports to the all-source system only after ensuring all technical channels measures for reporting have been met.

3951
3952
3953
3954

6-26. The *2X is a commissioned officer with a CI or HUMINT area of concentration (AOC) (35E/F). Within joint and combined force commands, the C/J2X may be either an Army, Navy, Air Force or Marine officer or civilian depending upon the requirements of the approved joint manning document. (See TC 2-22.303 for details on the 2X.)



3955

Figure 6-1. 2X organization

3956

COUNTERINTELLIGENCE COORDINATING AUTHORITY

3957
3958

6-27. The CICA is the coordinating authority for all CI activities for all assigned or attached Army CI assets. The CICA for Army Divisions and Corps will normally be a senior 351L CI warrant officer (WO).

FOR OFFICIAL USE ONLY

3959 At the ASCC, the CICA may be a senior CI WO, CI officer (35E) or equivalent Military Intelligence
3960 Civilian Excepted Career Program government civilian employee.

3961 6-28. Within Joint and multinational force commands, the TFCICA may be either an Army, Navy, Air
3962 Force, or Marine WO, officer, or civilian depending upon the requirements of the approved Joint Manning
3963 Document. Army CICA components generally consist of four personnel (a CI WO and three enlisted CI
3964 Soldiers); however, size and structure may vary depending upon the unit and mission. Units engaged in
3965 operational and strategic missions may also have a higher standard of grade for CICA's to include the use of
3966 appropriately credentialed government civilian employees. CICA personnel may be assigned, attached, or
3967 under operational control (OPCON).

3968 6-29. Regardless of echelon or service component, the CICA's mission is to manage, coordinate, and
3969 synchronize all CI activities in the designated area of intelligence responsibility. The CICA exercises
3970 technical channels for all CI entities and deconflicts CI activities with higher, lower, and adjacent CI
3971 elements. The CICA accomplishes all responsibilities through coordination with the operational units and
3972 other 2X staff elements. (See TC 2-22.303 for details on the CICA.)

3973 6-30. The CICA performs the following functions:

- 3974 ● Is responsible for coordinating and staffing all CI FP source operations (CFSO) proposals with
3975 the Army Component or JTF approval authority and US national agency representatives.
- 3976 ● Serves as the single focal point for all matters associated with CI in the area of intelligence
3977 responsibility. The CICA tracks CI activities and keeps the 2X informed so the 2X in turn can
3978 keep the C/J/G/S-2 and commander informed.
- 3979 ● Exercises technical authority of all CI entities and coordinates all CI activities in the area of
3980 intelligence responsibility. Coordinates with MI unit commanders who possess CI assets that
3981 execute CI activities in the area of intelligence responsibility.
- 3982 ● Coordinates and deconflicts all CI source operations with the source registry manager in the area
3983 of intelligence responsibility.
- 3984 ● Ensures a robust CI Education and Awareness Training Program by coordinating Subversion
3985 and Espionage Directed Against the Army (SAEDA) refresher training, as required, and by
3986 ensuring the establishment of SAEDA reporting channels and procedures in the area of
3987 intelligence responsibility.
- 3988 ● Is responsible for implementation of the intelligence program for all CI activities in the AO in
3989 accordance with AR 381-10.

3990 *Note.* The military departments always remain in control of CI investigations. The Army Theater
3991 CI Coordinating Authority (ATCICA) and Army CI Coordinating Authority (ACICA) provide
3992 investigative technical channels for all Army CI conducted investigations. While Army CI
3993 investigative reports will pass through the CICA and *2X, they will go simultaneously to the
3994 ATCICA and ACICA.

- 3995 ● Keeps the 2X, C/J/G/S-2, and commander informed on the status of CI activities.
- 3996 ● Coordinates with the analytical element and with the ISR synchronization staff to identify and
3997 refine requirements for CI collection, operations, or investigations.
- 3998 ● Ensures CI reporting is disseminated to the analytical element for inclusion into all-source
3999 analysis, as appropriate.
- 4000 ● Develops and disseminates requirements, orders, and RFIs to CI entities in the area of
4001 intelligence responsibility.
- 4002 ● Ensures registration of all CI sources with the OSC or other designated source registry manager.
4003 (If there is no OSC, the CICA will maintain the source registry.)
- 4004 ● Routinely evaluates CI source operations to ensure proper handling by CI Special Agents,
4005 source ability to satisfy requirements, and to determine value of continuing the operation.

FOR OFFICIAL USE ONLY

- 4006 ● Ensures exploitation opportunities are preserved while conducting vulnerability assessments and
4007 other FP initiatives.
- 4008 ● Ensures investigations are planned, prepared, executed, and assessed in accordance with
4009 applicable directives and regulations.
- 4010 ● Establishes and maintains connectivity with the supporting ATCICA for investigative oversight
4011 for Army CI-conducted investigations.
- 4012 ● Participates in the operations staff targeting process to provide input on the placement, access,
4013 availability of sources, and reporting reliability of CI sources that support operations.
- 4014 ● Ensures CI support is provided to the JIDC and detainee holding areas in the area of intelligence
4015 responsibility.
- 4016 ● Establishes quality control and executes release for all CI reporting.
- 4017 ● Routinely provides feedback to all CI entities in the area of intelligence responsibility regarding
4018 their collection activities, operations, and investigations.
- 4019 ● After a determination has been made to release a detainee, ensures screening is performed of the
4020 detainee to be released to determine the detainee's suitability as a potential lead for CI or other
4021 collection activities.
- 4022 ● Interacts with the HOC and OSC to ensure CI activities do not conflict with HUMINT activities
4023 in the area of intelligence responsibility.
- 4024 ● Conducts liaison with the Provost Marshal Office and intelligence entities conducting liaison
4025 with HN LEAs to ensure CI activities are coordinated and deconflicted.
- 4026 ● Conducts liaison with HN and US national level CI organizations.
- 4027 ● Provides staff oversight to locally employed personnel (LEP) screening activities within the area
4028 of intelligence responsibility.
- 4029 ● Provides technical oversight and guidance for requests for coordination or approval for CI
4030 operations which require approvals outside the local approval authority.
- 4031 ● Recommends to the supported C/J/G/S-2 and maneuver commander the designation of an MI
4032 unit or intelligence staff element, as appropriate, to serve as the repository for CI Badge and
4033 Credentials in the area of intelligence responsibility with responsibility for accountability and
4034 issue of CI Badge and Credentials.
- 4035 ● Coordinates requests for CI technical services (cyber CI unit, TSCM, and polygraph support).

4036 COUNTERINTELLIGENCE OPERATIONAL MANAGEMENT TEAM

- 4037 6-31. The OMT is the first operational management element that provides technical channels to
4038 subordinate CI teams. The OMT manages subordinate CI teams to ensure operational execution and
4039 direction, quality and control of reporting, and satisfaction of intelligence requirements. An OMT can
4040 manage between one to four CI teams depending on the operational tempo mission and geographic
4041 requirements. OMTs generally consist of four personnel (a 351L, CI WO and three 97L, CI enlisted
4042 Soldiers); however, size and structure may vary depending upon the unit and mission.
- 4043 6-32. Units engaged in operational and strategic missions may also have a higher standard of grade for
4044 OMTs to include the use of appropriately credentialed government civilian employees. OMT personnel
4045 may be organic, attached, or assigned under OPCON. OMTs and subordinate CI teams may be pushed
4046 down from higher echelon units to lower echelon units. Depending upon mission requirements, CI OMTs
4047 may be held at the next higher echelon of the subordinate CI teams. CI OMTs will normally never be
4048 located below the brigade level. (See TC 2-22.303 for details on the OMT.)
- 4049 6-33. The OMT performs the following functions:
- 4050 ● Is responsible for passing all intelligence or time-sensitive information to the command channels
4051 for action.
 - 4052 ● Provides guidance and technical channels for operational activity.

FOR OFFICIAL USE ONLY

- 4053 ● Provides the collection focus and operational focus for CI teams.
- 4054 ● Provides quality control and dissemination of reports for subordinate CI teams; receives, edits,
- 4055 and provides feedback on all administrative reports (for example, resource status reports),
- 4056 operational reports (for example, contact reports), and intelligence reports (for example,
- 4057 intelligence information reports) provided by subordinate teams.
- 4058 ● Ensures that CI reporting and related traffic from above and below are fused into the all-source
- 4059 picture.
- 4060 ● Conducts CI analysis and assists in mission analysis for the supported commander.
- 4061 ● Coordinates CI activities with the CICA and with CI element commanders in the area of
- 4062 intelligence responsibility.
- 4063 ● Performs liaison with HN and US national level security, intelligence, and law enforcement
- 4064 organizations.
- 4065 ● Informs respective CICA when Army CI elements are conducting CI investigative activities
- 4066 within the purview of AR 381-20.
- 4067 ● Acts as a conduit between subordinate CI teams, the CICA and 2X, and the supported unit
- 4068 headquarters.
- 4069 ● Provides administrative support for subordinate CI teams to include reporting mission and
- 4070 equipment status to the CICA or HOC and the supported unit headquarters.
- 4071 ● Educates the supported commander on the capabilities of subordinate teams.
- 4072 ● Integrates subordinate CI teams directly into the unit's ISR planning.

4073 **COUNTERINTELLIGENCE TEAM**

- 4074 6-34. The CI team conducts CI investigations, CI operations, CI collection (debriefings, source operations,
- 4075 liaison, and screening), CI analysis, and CI technical services support to protect the supported unit from
- 4076 threat intelligence activities.
- 4077 6-35. The CI team provides the supported commander, through 2X channels, a capability to help protect
- 4078 the force and affect the adversaries' understanding of friendly force operational capabilities. The CI team
- 4079 also provides a capability to help answer PIRs related to AFIST collection activities targeted against the
- 4080 supported unit, US Army, and DOD equities.
- 4081 6-36. A CI team generally consists of four 35L, CI noncommissioned officers (NCOs) and enlisted
- 4082 Soldiers. Units engaged in higher echelon missions may also have a higher standard of grade for CI teams
- 4083 to include the use of appropriately credentialed government civilian employees. Specialized CI teams, to
- 4084 include technical counterintelligence, cyber CI and polygraph, may vary in composition (2- to 3-person
- 4085 military and/or civilian teams) based upon mission requirements and unit organization. CI teams—
- 4086 ● May be assigned, attached, or OPCON.
 - 4087 ● May be pushed down from higher echelon units to lower echelon units.
 - 4088 ● May be pushed down to brigade level depending upon mission requirements.
- 4089 6-37. The CI team performs the following functions:
- 4090 ● Prepares and submits command reports, such as readiness status reports that provide status of
 - 4091 equipment, personnel, and intelligence contingency funds in accordance with supporting OMT
 - 4092 SOPs.
 - 4093 ● Prepares protected reports, such as contact reports, in accordance with OMT SOPs, that
 - 4094 document each source contact.
 - 4095 ■ Disseminates contact reports to their supporting OMT for review or comment.
 - 4096 ■ Maintains contact report files on every source.
 - 4097 ■ Provides contact report files to replacing team during relief in place or transfer of authority.

FOR OFFICIAL USE ONLY

- 4098 ● Prepares and submits intelligence reports, such as SPOT reports using the SALUTE (size, activity, location, unit, time, equipment) format and intelligence information reports in accordance with OMT SOPs.
- 4099
- 4100
- 4101 ● Assists in the production of threat assessments and vulnerability assessments. This function provides support to evaluations of installations and operating bases in conjunction with MP, CA, engineers, and medical units to identify the intelligence threat to the operating location. The vulnerability assessment identifies weaknesses in operational and physical security procedures and recommends countermeasures to mitigate intelligence collection on friendly forces; this limits the ability of adversaries to plan and conduct hostile acts on US and multinational activities and locations.
- 4102
- 4103
- 4104
- 4105
- 4106
- 4107
- 4108 ● Conducts CI analysis to support mission requirements and contributes to the COP. To verify adequate area coverage, uses backwards planning and source profiling to choose CI targets.
- 4109
- 4110 ● Develops and uses CI target overlays and other CI analytical tools that illustrate the CI situation, identify CI gaps, and help refocus CI collection efforts.
- 4111
- 4112 ● Conducts CI debriefings. This function involves the systematic questioning of individuals to procure information to answer specific CI collection requirements by direct and indirect questioning techniques. Sources for debriefing include friendly forces (for example, MP, CA, engineers, and medical units), US and non-US civilians to include members of NGOs, refugees, displaced civilians, and local inhabitants. The supported S-2, with the help of the CI team, regularly and systematically debriefs all ISR assets.
- 4113
- 4114
- 4115
- 4116
- 4117
- 4118 ● Conducts CI investigations within the jurisdictional boundaries of Army CI regulations and the guidelines of AR 381-10, AR 381-12 and AR 381-20. Regularly coordinates with the supporting staff judge advocate to ensure investigations are conducted in such a way as to support eventual trial and prosecution, if necessary, and to be in compliance with all DOD policy and US laws.
- 4119
- 4120
- 4121
- 4122 ● Conducts CI screening.
- 4123 ● Conducts CI collection.
- 4124 ● Registers all CI contacts through the OMT and CICA in the source registry. Disseminates CI administrative, technical, and intelligence reports through the OMT and CICA.
- 4125
- 4126 ● Conducts CI liaison with US, multinational, and HN military and civilian agencies, to include NGOs, for the purpose of obtaining information of CI interest and to coordinate and deconflict CI activities. Liaison activities are designed to ensure a cooperative operating environment for CI elements and to develop CI leads for further exploitation.
- 4127
- 4128
- 4129
- 4130 ■ Maintains constant contact with the supported S-2 in order to identify intelligence requirements and information gaps and to deconflict operations within the support commander's AO.
- 4131
- 4132
- 4133 ■ Maintains constant contact with other ISR assets in order to coordinate and deconflict operations in adjacent AOs and cross-checks collected information.
- 4134
- 4135 ● Supports the CI Education and Awareness Training Program by coordinating with the S-2 of all units in their area of intelligence responsibility to present SAEDA awareness training. CI teams should be the focal point for all SAEDA training in order to identify incidents of CI interest and educate Army personnel concerning their responsibilities to report incidents that are outlined in AR 381-12. The CI Education and Awareness Training Program supports the commander's overall FP program.
- 4136
- 4137
- 4138
- 4139
- 4140
- 4141 ● Provides CI technical service support (for example, TSCM, polygraph, computer forensics) to the supported unit when properly trained and equipped personnel are provided.
- 4142

4143 **ARMY COUNTERINTELLIGENCE LEVELS OF EMPLOYMENT**

- 4144 6-38. CI is critical to Army operations at all echelons, during peacetime and throughout the full spectrum of operations. The only difference in the operational execution is generally what mission areas are being
- 4145

FOR OFFICIAL USE ONLY

4146 supported. Even CI Special Agents providing CI technical services and support are leveraged to provide
4147 their unique capabilities during peacetime and during garrison and during deployed operations.

4148 6-39. Due to the transformation of CI to a HUMINT collection function in recent operations, the true
4149 mission and proper employment of CI as a warfighting enabler need to be articulated to commanders.

4150 **STRATEGIC AND DEPARTMENTAL**

4151 6-40. Strategic operations are conducted by CI elements supporting national and DOD missions (for
4152 example, support to North Atlantic Treaty Organization and special operations and missions). Strategic CI
4153 also conducts compartmented investigations and operations to affect the knowledge of adversarial
4154 intelligence regarding contingency operations (CONOPs) and defense information. Strategic CI executes
4155 the full range of CI functions and missions including CI investigations and operations, OFCO, research and
4156 technology protection, SAP support, treaty verification, and technical CI services (polygraph, TSCM, and
4157 computer forensics). Strategic CI also supports SOF and special mission units within the scope of
4158 applicable national, DOD, and DA policies and regulations. Strategic and departmental CI assets generally
4159 conduct the following activities:

- 4160 ● **Advice and Assistance.** Assists unit security managers and commanders with knowledge on
4161 security programs and provides details on reporting potential AFIST targeting and incidents of
4162 CI interest.
- 4163 ● **Education and Awareness.** Provides AFIST threat and US Army program briefings to educate
4164 unit personnel, satisfy mandatory training requirements, and generate potential leads for
4165 incidents of CI interest.
- 4166 ● **Target Acquisitions and Vulnerability Assessments.** Conducts collection and analysis of
4167 AFIST threat data for a specific unit, facility, operation, or activity to provide the supported
4168 commander knowledge on FP and security posture and make countermeasures recommendations
4169 to overcome deficiencies.
- 4170 ● **CI Investigations.** Exploits or neutralizes potential AFIST collection threats targeting US Army
4171 and DOD equities.
- 4172 ● **CI Collection.** Detects and identifies AFIST intelligence collection activities targeting US
4173 forces and devises other CI initiatives to counter, exploit or neutralize the AFIST collection
4174 capability.

4175 **Army G-2X**

4176 6-41. At the departmental level the Army G-2X is the executive agent for all Army CI activities to include
4177 policy implementation, operational oversight, intelligence funding programs, and Army staff level
4178 management. The Army G-2X—

- 4179 ● Coordinates with other military service and national agency intelligence and CI services to
4180 coordinate CI strategies and mutually supporting activities, to include joint CI operations and
4181 investigations.
- 4182 ● Is responsible for making recommendations to the DA G-2 concerning all budgetary issues
4183 concerning CI and HUMINT.
- 4184 ● Provides oversight and guidance for Army CI elements. It staffs and coordinates approval of CI
4185 Operational Concepts and Plans as outlined AR 381.20, chapter 2, to ensure they meet legal
4186 sufficiency and satisfy validated requirements and provides oversight for all approved Army CI
4187 Operational Concepts and Plans.
- 4188 ● Manages and maintains the Army's centralized CI and HUMINT source registry and product
4189 library as part of a Joint Service CI and HUMINT database.
- 4190 ● Coordinates functional and technical support services, as well as comprehensive worldwide
4191 AFIST threat analysis products.

FOR OFFICIAL USE ONLY

- 4192 ● Collaborates with CI staffs and field elements at all echelons to ensure unity of the CI effort and
4193 efficient use and employment of Army CI assets.

4194 **Army Counterintelligence Coordinating Authority**

- 4195 6-42. The ACICA is subordinate to the Army G-2X and is responsible for implementing and enforcing US
4196 and DOD policy within the Army and providing technical channels for all Army CI Activities.
4197 The ACICA—
- 4198 ● Reviews, staffs, and coordinates all special investigative and collection techniques requested by
4199 Army CI elements. The ACICA—
 - 4200 ● Is responsible for approving all Army CI investigations.
 - 4201 ● Reviews, staffs, and coordinates all CI operational plans and concepts with the appropriate
4202 agencies and approval authorities.
 - 4203 ● Coordinates with other US government and military CI agencies to assist in the development
4204 and implementation of national CI strategies.

4205 **Intelligence and Security Command**

- 4206 6-43. INSCOM executes departmental and operational CI activities in accordance with guidance from the
4207 Army G-2X. INSCOM has the responsibility for administrative C2 of all Army Theater Military
4208 Intelligence Brigades (MIBs) supporting their respective theater ASCC. INSCOM CI assets are task-
4209 organized and operationally employed based upon mission and geographic requirements. Most MIBs
4210 organize their CI assets into detachments with subordinate field or resident offices.

4211 **OPERATIONAL**

- 4212 6-44. These CI assets are generally assigned to ASCC and are generally focused on a specific theater. CI at
4213 the operational level is primarily focused on counterespionage and CI support to FP. Operational CI assets
4214 are instrumental in protecting bases of operations from infiltration, collection, planning, and targeting by
4215 AFIST entities. Although operational CI elements have a vital mission to counter the AFIST threat on a
4216 daily basis, they may be tasked to deploy and support contingency or combat operations. This is especially
4217 true in major combat operations when the size, scale, and scope of the operation exceed the capability of
4218 organic tactical CI assets to provide adequate support in the AO. Operational CI assets may also be tasked
4219 to support strategic CI operations when required. Operational CI assets generally conduct the following
4220 activities:
- 4221 ● **Advice and Assistance.** Assists unit security managers and commanders with knowledge on
4222 security programs and provides details on reporting potential AFIST targeting and incidents of
4223 CI interest.
 - 4224 ● **Education and Awareness.** Provides AFIST threat and SAEDA briefings to educate unit
4225 personnel, satisfy mandatory training requirements, and generate potential leads for incidents of
4226 CI interest.
 - 4227 ● **Threat Assessments and Vulnerability Assessments.** Conduct collection and analysis of
4228 AFIST threat data for a specific unit, facility, operation, or activity to provide the supported
4229 commander knowledge on FP and security posture and make countermeasures recommendations
4230 to overcome deficiencies.
 - 4231 ● **CI Screening.** Vets LEP in overseas and deployed locations for suitability to work, FP
4232 liabilities, associations, or contacts that may allow them to be used in other CI collection
4233 initiatives.
 - 4234 ● **CI Investigations.** Exploits or neutralizes potential AFIST collection threats targeting US Army
4235 and DOD equities.

FOR OFFICIAL USE ONLY

- 4236 ● **CI Collection.** Detects and identifies AFIST intelligence collection activities targeting US
4237 forces and to devise other CI initiatives to counter, exploit, or neutralize the AFIST collection
4238 capability.

4239 **Theater G-2X**

- 4240 6-45. The Theater G-2X is the principal advisor to the theater ASCC G-2 and commander for all CI and
4241 HUMINT matters. The theater G-2X consists of the G-2X staff officer, theater HOC, ATCICA, and OSC.
4242 The theater G-2X—
- 4243 ● Provides guidance and oversight based upon Army G-2X directives and theater requirements.
 - 4244 ● Provides technical channels and operational coordination for all theater Army CI and HUMINT
4245 elements.
 - 4246 ● Also coordinates technical support services, source registration and national level product
4247 support with the Army G-2X. Regional analysis and production is provided to theater consumers
4248 and forwarded to the Army G-2X for inclusion into the national database.

4249 **Army Theater Counterintelligence Coordinating Authority**

- 4250 6-46. The ATCICA is subordinate to the Theater G-2X and is responsible for providing guidance and
4251 technical channels for all Army CI collection and investigative and operational activities within their
4252 theaters of operation, to include CI elements assigned to tactical organizations. ATCICA—
- 4253 ● Is responsible for reviewing and staffing all requests for special investigative and collection
4254 techniques and investigative and operational plans and concepts.
 - 4255 ● Is the interface between subordinate Army CI operational management elements and the
4256 ACICA.
 - 4257 ● Is responsible for implementing Army CI policy as directed by the ACICA and Army G-2X.
 - 4258 ● Conducts liaison with other US government and military, HN intelligence, security, and LEAs to
4259 coordinate and deconflict CI activities.

4260 **Military Intelligence Brigade**

- 4261 6-47. MIBs provide operational support to the separate ASCCs. CI elements in MIB support CCDRs,
4262 generally in combatant commander's AORs. Operational level CI activities and functions include
4263 investigations, collection, analysis and production, and technical services and support. CI elements must be
4264 capable of quickly transitioning from a peacetime mission to crisis operations to support CCDR
4265 requirements. Theater CI assets conduct Army, joint, and multinational operations in their JOAs.
4266 Operational elements may also be deployed to support or reinforce tactical forces in CONOPs.

4267 **TACTICAL**

- 4268 6-48. Tactical CI generally denotes all CI assets assigned to Army corps and below. This includes CI
4269 assigned directly to brigade combat teams, divisions, and corps units. CI at the tactical level is primarily
4270 focused on CI support to FP to their supported commanders during contingency and combat operations or
4271 to the war on terrorism. CI assets at the tactical level are instrumental in protecting bases of operations
4272 from infiltration, collection, planning, and targeting by AFIST entities.

- 4273 6-49. Tactical CI assets generally do not have a robust peacetime mission since their focus is providing
4274 support to their combat arms parent organization; however, in some cases operational and strategic CI
4275 elements may formally request their support on a case-by-case basis or through formal written agreements.
4276 Even during peacetime garrison operations, tactical CI assets are essential in providing advice and
4277 assistance to their supported command and other CI operational activities that can assist and be the
4278 instigator for more complex CI initiatives. Depending upon the size, scale, and scope of ongoing

FOR OFFICIAL USE ONLY

4279 operations, operational and strategic CI assets may also be tasked to augment tactical operations. CI assets
4280 assigned to tactical units generally conduct the following activities:

- 4281 ● **Advice and Assistance.** Assists unit security managers and commanders with knowledge on
4282 security programs and provides details on those CI assets that can respond to AFIST targeting.
- 4283 ● **Education and Awareness.** Provides AFIST threat and SAEDA briefings to educate unit
4284 personnel, satisfy mandatory training requirements, and generate potential leads for CI elements
4285 chartered to conduct investigations during peacetime.
- 4286 ● **Threat Assessments and Vulnerability Assessments.** Conducts collection and analysis of
4287 AFIST threat data for a specific unit, facility, operation, or activity to provide the supported
4288 commander knowledge on FP and security posture and make countermeasures recommendations
4289 to overcome deficiencies.
- 4290 ● **CI Screening.** Vets LEPs in overseas and deployed locations for suitability to work, FP
4291 liabilities, associations, or contacts that may allow them to be used in other CI collection
4292 initiatives.
- 4293 ● **CI Investigations.** Identifies potential CI investigation requirements and triages those incidents
4294 for other CI assets chartered to conduct the investigation. This can be accomplished during
4295 peacetime and contingency or combat operations. During contingency or combat operations, the
4296 chartered CI element may request the assistance of tactical CI personnel to fulfill investigative
4297 requirements. Tactical CI assets generally do not have the resources to effectively execute a
4298 complex CI or counterespionage investigation.
- 4299 ● **CI Collection.** Detects and identifies AFIST intelligence collection activities targeting US
4300 forces and devises other CI initiatives to counter or neutralize the AFIST collection capability.
4301 CI collection is only conducted in contingency or combat operational environments and when
4302 approved by the CICA.

4303 Corps/Division/Brigade G-2X

4304 6-50. The G/S2X is the principal advisor to their supported commander for all CI and HUMINT matters
4305 within their area of intelligence responsibility. The G/S2X consists of the G/S2X staff officer, HOC, and
4306 the CICA. At lower echelons (for example, Stryker Brigade Combat Team and brigade combat team
4307 levels), an OSC may not be authorized or resourced and may have to be task-organized from assigned and
4308 attached resources in order to provide this capability.

4309 6-51. The G/S2X provides direct technical channels for all CI and HUMINT assets within their unit and
4310 area of intelligence responsibility. The G/S2X—

- 4311 ● Coordinates and deconflicts all CI and HUMINT activities between higher, lower, and adjacent
4312 *2X elements.
- 4313 ● Is responsible for providing and maintaining a consolidated source registration for all CI and
4314 HUMINT elements within their area of intelligence responsibility and providing source data to
4315 the next higher echelon *2X element.
- 4316 ● Coordinates requests for technical support services, source registration, and higher level
4317 analytical support with the next higher echelon *2X element.
- 4318 ● Must have knowledge of the CI and HUMINT resources and capabilities for all military, DIA,
4319 and US Government agencies. The G-2X must be able to transition from an Army Force
4320 operation to functioning as a J-2X if their unit is designated as a JTF headquarters.

4321 Corps or Division CICA

4322 6-52. The Corps or Division CICA are directly subordinate to their respective Corps or Division G-2X
4323 element. The CICA provides direct oversight and control for all CI activities within their supported unit
4324 and area of intelligence responsibility. The CICA is responsible for coordinating and deconflicting all CI
4325 activities with the next higher echelon CICA. It conducts liaison with other US Government and military

FOR OFFICIAL USE ONLY

4326 and HN intelligence, security, and LEAs within their area of intelligence responsibility to coordinate and
4327 deconflict CI activities. The CICA—

- 4328 ● Reviews and provides quality control and dissemination of all CI reporting from subordinate CI
4329 elements.
- 4330 ● Provides operational analysis to focus CI activities, assess responsiveness and effectiveness of
4331 CI activities, and ensures coverage of information requirements for their supported commander.
- 4332 ● Must have knowledge of the CI resources and capabilities for all military, DIA, and US
4333 Government agencies.
- 4334 ● Must be able to transition from an Army Force operation to functioning as a TFCICA if their
4335 unit is designated as a JTF headquarters.

4336 **Corps or Division CI Elements**

4337 6-53. CI assets supporting division and JTF operations are generally leveraged from tactical battlefield
4338 surveillance brigades (BFSBs). The G-2X at division will provide CI investigation and technical channels
4339 for CI elements supporting division elements. The division G-2X will coordinate CI activities through the
4340 JTF J-2X in theater and their theater CICA and/or senior CI staff officer. The Division G-2X must be
4341 trained and equipped to act as a J-2X in the event the division is designated as the JTF command element
4342 during a CONOP.

4343 6-54. At corps or division level, the BFSB battalion has three companies with CI assets. The collection and
4344 exploitation (C&E) company has one CI OMT that controls three CI teams. Each CI team consists of four
4345 enlisted CI Soldiers. The C&E company's mission is to provide general support coverage for the division.
4346 Each of the two CI and HUMINT companies has two CI teams and no CI OMTs. The CI and HUMINT
4347 company's mission is to provide its assets in DS to the BCTs.

4348 **Brigade Combat Team**

4349 6-55. Within a BCT there are no organic CI OMTs or CI teams in the MI company. CI support pushed
4350 down to the BCT must include an OMT or be controlled by the BCT S-2X/CICA. CI teams pushed down
4351 to the BCT conduct operations in a DS role throughout the brigade's AOR during contingency or combat
4352 operations.

4353 **JOINT OPERATIONS**

4354 6-56. In a joint or combined operation, the J-2X and the TFCICA are the senior authorities for the conduct
4355 of all CI agencies involved in the operation. All subordinate Army G/S-2X and CICA's will coordinate and
4356 deconflict their CI and HUMINT activities with the senior JTF J-2X and TFCICA. In a JTF, DOD policy
4357 and joint doctrine will be the basis for the conduct of all CI operations throughout the joint operational
4358 environment.

4359 6-57. Subordinate Army element CI assets may use service specific doctrine for guidance but must ensure
4360 that activities are conducted within the parameters established by the JTF. The separate military
4361 departments always remain in control of CI investigations. The ACICA provides investigative technical
4362 channels for all Army CI-conducted investigations. While Army CI investigative reports will pass through
4363 the CICA and *2X, they will go simultaneously to the ATCICA and ACICA.

4364 **SUPPORT TO CONTINGENCY OPERATIONS**

4365 6-58. The initial phase of operations from peacetime military engagement to major theater war lays the
4366 foundation of future team operations. In general, the priority of effort focuses inward on security of
4367 operating bases, areas of troop concentration, and C2 nodes to identify the collection threat to US forces
4368 that could be used by adversary elements to plan hostile acts against US activities and locations.

FOR OFFICIAL USE ONLY

4369 6-59. Once security of the operating bases has been established, the operational focus of CI teams shifts
 4370 outside the operating base to continue to detect, identify, and neutralize the collection threat to US forces
 4371 as well as to provide I&W of hostile acts targeting US activities. The CI team uses several collection
 4372 methods, to include CFSO, elicitation, and liaison, to answer the supported commander's requirements.
 4373 This is referred to as the continuation phase. The CI team conducts CI investigations to identify, neutralize,
 4374 and exploit reported threat intelligence collection efforts.

4375 6-60. A key element to the CI team's success is the opportunity to spot, assess, and develop relationships
 4376 with potential sources of information. Operating as independent teams, without being tied to ISR or combat
 4377 assets, enables the CI team's maximum interaction with the local population, thereby maximizing the pool
 4378 of potential sources of information. Along with the opportunity to spot, assess, and interact with potential
 4379 sources of information, a second key element of a CI team's success is its approach ability to the local
 4380 population. A soft posture enables a CI team to appear nonthreatening. Experience has shown that the local
 4381 population in general is apprehensive of fully and openly armed patrols and Soldiers moving around
 4382 population centers.

4383 6-61. During some operations, civilian attire or nontactical vehicles may be used to lower the CI team
 4384 profile. In some special situations, these measures are taken to make the operation less visible to the casual
 4385 observer. Also, in some cultures, sharing food and beverages among friends is expected; exceptions to
 4386 restrictions or general orders should be considered to facilitate successful CI team operations, many of
 4387 which are geared towards developing relationships with potential sources of information.

4388 **SUPPORT TO INSTALLATIONS AND OPERATING BASES**

4389 6-62. CI teams, as part of a multi-agency team consisting of MPs, CA, medical, and explosive ordnance
 4390 disposal, support the conduct of threat assessments and vulnerability assessments of installations and
 4391 operating bases to identify the intelligence threat to the operating locations. Detailed threat assessments and
 4392 vulnerability assessments identify weaknesses in operational and physical security procedures and
 4393 recommend countermeasures to mitigate intelligence collection on friendly forces. Threat assessments and
 4394 vulnerability assessments limit the ability of the threat to plan hostile acts on US activities and locations. CI
 4395 activities supporting installations and operating bases include—

- 4396 ● Interviewing walk-in sources and LEP.
- 4397 ● Screening LEP. Commanders, staff planners, and G-2/S-2s should always provide input to
 4398 personnel assigned to establish and negotiate contracts using LN hires. This requirement ensures
 4399 that LN hires can be screened, interviewed, and in some instances used as CI sources or assets in
 4400 order to provide intelligence information that impacts the security of the base camp.
- 4401 ● Debriefing friendly force personnel who are in contact with the local population, such as—
 4402 ■ ISR patrols.
 4403 ■ MP patrols.
 4404 ■ Combat patrols.
 4405 ■ Liaison personnel.
 4406 ■ CA and PSYOP teams.
- 4407 ● Conducting limited local open-source information collection.
- 4408 ● Providing support to threat assessments and vulnerability assessments of the base camp.

4409 **OPERATIONAL CONSIDERATIONS**

4410 6-63. CI must be represented and integrated into all phases of operational planning. The success of a CI
 4411 team is measured by the operational emphasis, resourcing, and equipping they receive from their supported
 4412 command. While operational security and freedom of movement are critical to effective CI operations,
 4413 conditions within the AO—specifically high threat areas—will often require the CI team to find non-

FOR OFFICIAL USE ONLY

4414 doctrinal solutions to allow them to operate. This may mean the CI team is paired with other combat and
4415 non-combat units to facilitate movement in a particular AO.

4416 6-64. The mission of the CI team must be integrated into the overall scheme of maneuver in order to
4417 support the commander's requirements. CI teams are often resourced or outfitted with non-TOE
4418 equipment, resources, and personnel that serve a specific purpose and provide them a unique capability to
4419 support their commander. These resources should not be used for non-CI missions or redirected without
4420 the commander's approval; if this occurs, the commander is accepting a significant degradation to the
4421 unit's ISR capability.

4422 **TACTICS, TECHNIQUES, AND PROCEDURES**

4423 6-65. At the CI team level, team members conduct mission analysis and planning specific to their AO.
4424 Backwards planning and source profiling are used extensively to choose CI targets. To verify adequate
4425 area coverage, the CI team may periodically develop and use CI target overlays and other CI analytical
4426 tools that illustrate the CI situation, identify CI gaps, and help refocus the collection effort.

4427 6-66. The CI team is also in constant contact with the supported S-2 and the other ISR assets (Scouts,
4428 PSYOP, CA, and MP) in order to coordinate and deconflict operations and to cross-check collected
4429 information. The supported unit S-2, with the help of the CI team, regularly and systematically debriefs all
4430 ISR assets.

4431 6-67. The CI team must be integrated into the supported unit's ISR plan. The CI OMT chief will advise the
4432 supported unit on the specific capabilities and requirements of the team to maximize mission success.

4433 **OPERATIONAL RISK MITIGATION**

4434 6-68. The employment of CI teams includes varying degrees of contact with the local population. As the
4435 degree of contact with the population increases, both the quantity and quality of CI collection increases. In
4436 many instances, however, there is a risk to the CI team inherent with increased exposure to the local
4437 population. The decision at what level to employ a CI team is METT-TC dependent. The risk to the CI
4438 assets must be balanced with the need to collect on PIRs and to protect the force as a whole. ROE, SOFA,
4439 direction from higher headquarters, and the overall threat level may also restrict the deployment and use of
4440 CI teams.

4441 6-69. Risks are minimized through the situational awareness of CI team members. They plan and rehearse
4442 to readily react to any situation and carry the necessary firepower to disengage from difficult situations. If
4443 it becomes necessary to call for assistance, adequate and redundant communications equipment is critical.
4444 These scenarios and actions should be trained prior to deployment into a contingency area and rehearsed
4445 continuously throughout the deployment.

4446 6-70. A supported unit commander is often tempted to keep the CI team within friendly bases when the
4447 threat condition level increases. The supported commander must weigh the risk versus potential
4448 information gain when establishing operational parameters of supporting CI teams. This is necessary
4449 especially during high threat condition (THREATCON) levels when the supported unit commander needs
4450 as complete a picture as possible of the threat arrayed against US and multinational forces.

4451 6-71. When it is not expedient to deploy the CI team independently due to THREATCON levels or other
4452 restrictions, the team can be integrated into other ongoing operations. The CI team may be employed as
4453 part of a combat, ISR, or MP patrol or used to support CA, PSYOP, engineer, or other operations. This
4454 method reduces the risk to the team while allowing a limited ability to collect information. It also has the
4455 advantage of placing the team in contact with the local population and allowing it to spot, assess, and
4456 interact with potential sources of information. However, this deployment method restricts collection by
4457 subordinating the team's efforts to the requirements, locations, and timetables of the unit or operation into
4458 which it is integrated and does not allow for the conduct of sensitive source operations.

FOR OFFICIAL USE ONLY

4459 *Note.* This method of employment should be considered a last resort.

4460 **INTEGRATION OF LINGUISTS**

4461 6-72. Integrating linguists into the CI team should take place as soon as possible. Security clearances and
4462 contractual agreements will help the team determine the level of integration.

4463 6-73. Along with the basic briefing of what is expected of the civilian linguists as interpreters, CI teams
4464 should be informed about civilian chain of command and the scope of their duties beyond interpreting. The
4465 CI team leader must ensure that linguists are trained and capable of completing all tasks expected of them.

4466 **COUNTERINTELLIGENCE EQUIPMENT**

4467 6-74. Basic C2, transportation and weapons requirements do not differ significantly from most Soldier
4468 requirements and are available as unit issue items. However, CI teams have unique communications,
4469 collection, processing, and mission-specific requirements.

4470 **COMMUNICATIONS**

4471 6-75. Dedicated and Secure Long-Range Communications. These are keys to the success of the CI team
4472 mission. CI team operations require a secure, three-tiered communications architecture consisting of inter-
4473 and intra-team radios, vehicle-based communications, and a CI and HUMINT base station.

4474 6-76. Communications Network. The CI team must have access to existing communications networks such
4475 as the tactical LAN. The CI team must also be equipped with its own COMSEC devices. It is imperative
4476 that the CI team acquire access to the public communication system of the HN. This can be in the form of
4477 either landlines or cellular telephones. Such access enables the CI team to develop leads which can provide
4478 early indicators to US forces.

4479 6-77. Interoperability. Communications systems must be equipped with an open-ended architecture to
4480 allow for expansion and compatibility with other service elements, government organizations, NGOs, and
4481 multinational elements to effectively communicate during CONOPs. All ISR systems must be vertically
4482 and horizontally integrated to be compatible across all warfighting functions and with all US Army
4483 organizations.

4484 6-78. Satellite Communications On The Move. To provide real-time and NRT information reporting, CI
4485 elements must have the capability to transmit voice, data, imagery, and video while on the move. CI teams
4486 must be able to transmit while geographically separated from their parent unit while operating remotely.
4487 This broadband requirement can only be achieved through a satellite communications capability and must
4488 be achievable while mobile.

4489 **CI COLLECTION AND PROCESSING SYSTEMS**

4490 6-79. The CI team must rely on automation to achieve and maintain information dominance in a given
4491 operation. With time, effective collection planning and management at all echelons, the CI team can collect
4492 a wealth of information. The processing and analysis of this information in a timely and efficient manner
4493 are crucial to operations. Automation helps the CI team to report, database, analyze, and evaluate the
4494 collected information quickly and to provide the supported unit with accurate data in the form of timely,
4495 relevant, accurate, predictive, and tailored intelligence.

4496 6-80. Automation hardware and software must be user friendly as well as interoperable among different
4497 echelons and services. They must interface with the communications equipment of the CI team as well as
4498 facilitate the interface of audiovisual devices. Technical support for hardware and software must be
4499 available and responsive.

FOR OFFICIAL USE ONLY

4500 6-81. The demand for accurate and timely CI reporting, DOMEX, and open-source information has grown
4501 tremendously. Biometric (physiological, neurological, thermal analysis, facial and fingerprint recognition)
4502 technologies will allow rapid identification, coding, and tracking of adversaries and human sources; as well
4503 as cataloging of information concerning EPWs, detainees, and civilians of CI interest on the battlefield.
4504 Biometrics will also provide secure authentication of individuals seeking network or facility access.

4505 6-82. CI teams work with multinational forces and other foreign nationals and require the ability to
4506 communicate in their respective languages. Often CI personnel have little or no training in the target
4507 language, and lack of skilled interpreters can hinder CI activities. CI teams require textual and voice
4508 translation devices, source verification, and deception detection machines (biometrics) to improve
4509 collection capability and accuracy.

4510 6-83. CI teams require dynamic machine language translation tools that provide both non-linguists and
4511 those with limited linguist skills a comprehensive, accurate means to conduct initial CI screenings and
4512 basic interviews in a variety of situations. CI elements will focus on in-depth interviews and
4513 communications with persons of higher priority. Machine language translation tools minimize reliance on
4514 contract linguists and allow Soldiers to concentrate on mission accomplishment.

4515 **MISSION SPECIFIC**

4516 6-84. In order to conduct night operations, each CI team member must be equipped with night vision
4517 devices, photographic equipment, and weapons. The CI team also may operate in urban and rural areas,
4518 where the threat level can vary from permissive to hostile. Some of the CI team missions may require the
4519 documentation of incidents. The CI teams can use the following equipment in their open-source collection
4520 efforts.

- 4521 ● Small, rugged, battery-operated digital camcorders and cameras which are able to interface with
4522 the collection and processing systems as well as communication devices.
- 4523 ● Global positioning systems that can be mounted and dismounted to move in the AO efficiently.
- 4524 ● Short-range multichannel RF scanning devices that can also identify frequencies which enhance
4525 their security.
- 4526 ● In some cases CI teams require a stand-off, high resolution optical surveillance and recording
4527 capability that can provide target identification at extended ranges to protect the intelligence
4528 collector while avoiding detection by the adversary target. An advanced optical capability
4529 provides intelligence collectors the ability to locate and track adversary targets (passive and
4530 hostile) for identification, collection, and target exploitations. High power, gyro-stabilized
4531 binoculars—which can be used from a moving vehicle—increase the survivability of the CI
4532 team and also give the team another surveillance and collection device.

4533

4534

4535

FOR OFFICIAL USE ONLY

4536

Chapter 7

4537

Human Intelligence

4538

HUMAN INTELLIGENCE-RELATED DEFINITIONS AND TERMS

4539

7-1. HUMINT is a category of intelligence derived from information collected and provided by human sources (JP 2-0).

4540

4541

7-2. A HUMINT source is a person from whom information is collected for the purpose of producing intelligence. HUMINT sources can include friendly, neutral, or hostile personnel. The source may either possess first- or second-hand knowledge normally obtained through sight or hearing. Categories of HUMINT sources include but are not limited to detainees, EPWs, refugees, displaced persons, local inhabitants, friendly forces, and members of foreign governmental and nongovernmental organizations (NGOs).

4542

4543

4544

4545

4546

4547

7-3. A HUMINT collector is a person who is trained to collect information from individuals (HUMINT sources) for the purpose of answering requirements. HUMINT collectors are the only personnel authorized to conduct HUMINT collection operations. They are trained and certified enlisted personnel in MOS 35M, warrant officers in MOS 351C and 351M, commissioned officers in MOS 35F, and their Federal civilian employee and civilian contractor counterparts. Trained means successful completion of one of the following courses, which are the only accepted sources of interrogation training for military personnel:

4548

4549

4550

4551

4552

4553

- 35M Basic HUMINT Collector Course at US Army Intelligence Center, Fort Huachuca, AZ.

4554

- US Marine Corps Basic Marine Air-Ground Task Force (MAGTF) CI/HUMINT Course at the Navy and Marine Corps Intelligence Center, Dam Neck, VA.

4555

4556

- Joint Interrogation Certification Course at HUMINT Training-Joint Center of Excellence, Fort Huachuca, AZ.

4557

4558

- Defense Intelligence Agency I-10 Course in Alexandria, VA.

4559

Note. Certification is conducted at the discretion of the Ccdr in accordance with established combatant command policies and directives.

4560

4561

7-4. HUMINT collection operations must be conducted in accordance with all applicable US law and policy. Applicable law and policy include US law; the law of war; relevant international law; relevant directives including DOD Directive 3115.09, DOD Directive 2310.1E, DOD instructions, FM 2-22.3, and military execute orders including fragmentary orders. Additional policies and regulations apply to the management of contractors engaging in HUMINT collection. (See FM 2-33.3, appendix K.)

4562

4563

4564

4565

4566

ROLE OF HUMAN INTELLIGENCE

4567

7-5. HUMINT operations focus on determining the capabilities, threat characteristics, vulnerabilities, and intentions of enemy and potential threat forces. The operations target actual and potential adversary decision-making architecture with the intent of helping to shape friendly forces' visualization of enemy and potential threat forces. HUMINT collection activities and operations include tactical questioning, screening, interrogation, debriefing, liaison, human source operations, DOMEX, and CEE operations.

4568

4569

4570

4571

FOR OFFICIAL USE ONLY

4572 7-6. Once the type of operation has been determined, leaders use the operations process of plan, prepare,
4573 execute, and assess to conduct the operation. The following paragraphs briefly discuss the different types
4574 of HUMINT operations.

4575 HUMINT COLLECTION METHODOLOGIES

4576 7-7. Every HUMINT questioning session, regardless of the methodology used or the type of operation,
4577 consists of five phases. The five phases of HUMINT collection are planning and preparation, approach,
4578 questioning, termination, and reporting. They are generally sequential; however, reporting may occur at
4579 any point within the process when critical information is obtained and the approach techniques used will be
4580 reinforced as required through the questioning and termination phases.

4581 7-8. HUMINT collection methodologies include five general categories:

- 4582 ● Screening.
- 4583 ● Interrogation.
- 4584 ● Debriefing.
- 4585 ● HUMINT Collection in Military Source Operations.
- 4586 ● Liaison.

4587 SCREENING OPERATIONS

4588 7-9. Screening is the process of evaluating and selecting human sources and documents for
4589 the prioritized collection of information based on the collection requirements and mission of
4590 the unit conducting the screening or its higher headquarters. Screening categorizes and
4591 prioritizes sources based on the probability of a particular source having priority information
4592 and the level of cooperation of the source. Screening is also used to determine if a source
4593 matches certain criteria that indicate that the source should be referred to another agency.
4594 Screening is conducted at all echelons of command and in all operational environments.
4595 There are two general categories of screening: human source screening, and document and
4596 media screening.

4597 7-10. Media is screened for content which answers PIRs or other information of intelligence interest.
4598 Screening operations also assist to determine which intelligence discipline or agency could best conduct
4599 the exploitation of a given source. Screening operations include, but are not limited to—

- 4600 ● Tactical screening in support of combat or contingency operations.
- 4601 ● Checkpoint screening (mobile or static) of local populations as they transit through and within
4602 the AO or to screen large numbers of individuals such as refugees or DP as they enter the AO.
- 4603 ● Local population screening of personnel within their own neighborhoods.
- 4604 ● Collection facility screening conducted as a normal part of HUMINT collection operations at
4605 collection facilities, such as theater interrogation and debriefing facilities and refugee camps.
- 4606 ● Local employee screening to determine possible security risks or identify sources who can
4607 provide information in response to CCIR.

4608 INTERROGATION OPERATIONS

4609 7-11. Interrogation is the systematic effort to procure information to answer specific collection
4610 requirements by direct and indirect questioning techniques of a person who is in the custody of the forces
4611 conducting the questioning. Some examples of interrogation sources include EPWs and other detainees.
4612 Interrogation sources range from totally cooperative to highly antagonistic. Interrogations may be
4613 conducted at all echelons in all operational environments.

4614 7-12. Detainee interrogation operations conducted at a Military Police (MP) facility, multinational-
4615 operated facility, or other agency-operated collection facility are more robust and require greater planning,

FOR OFFICIAL USE ONLY

4616 but have greater logistical support. Interrogations may only be conducted by personnel trained and certified
4617 in the interrogation methodology, including personnel in MOSs 97E, 351M (351E), or select others as may
4618 be approved by DOD policy. Interrogations are always to be conducted in accordance with the Law of
4619 War, regardless of the echelon or operational environment in which the HUMINT collector is operating.

4620 7-13. Interrogation operations are specific operations normally conducted at detainee collection facilities
4621 directed at the wide-scale collection of information from detainees using interrogation techniques.
4622 Although field interrogations are conducted at all echelons and during all operations in which there are
4623 detainees, detention facilities where interrogation operations occur are normally located only at theater or
4624 JTF level.

4625 **DEBRIEFING OPERATIONS**

4626 7-14. Debriefing is the systematic questioning of cooperating human sources to satisfy intelligence
4627 requirements consistent with applicable law. The source is usually not in custody and is usually willing to
4628 cooperate. Debriefing may be conducted at all echelons and in all operational environments. The primary
4629 categories of sources for debriefing are refugees, émigrés, displaced persons, local civilians, and friendly
4630 forces.

4631 **FRIENDLY FORCE DEBRIEFING OPERATIONS**

4632 7-15. Every member of the friendly force is a potential source for HUMINT collection. Friendly force
4633 personnel frequently have contact with the threat, civilian population, or the environment. Although many
4634 individuals report their information in the form of combat information, many do not report the information,
4635 do not realize its significance, or do not know how to report key information. Frequently a systematic
4636 questioning by a trained HUMINT collector will identify key information that can contribute to the
4637 intelligence picture and help an individual recall details. It also helps to place this information into a
4638 systematic format for the analyst to use.

4639 **HUMINT COLLECTION IN MILITARY SOURCE OPERATIONS**

4640 7-16. HUMINT collection in Military Source Operations (MSO) are directed toward the establishment of
4641 human sources who have agreed to meet and cooperate with HUMINT collectors for the purpose of
4642 providing information. Within the Army, MSO are conducted by trained personnel under the direction of
4643 military commanders. The entire range of HUMINT collection operations can be employed.

4644 7-17. MSO sources include one-time contacts, continuous contacts, and formal contacts from debriefings,
4645 liaison, and contact operations. MSO consist of collection activities that utilize human sources to identify
4646 attitude, intentions, composition, strength, dispositions, tactics, equipment, target development, personnel,
4647 and capabilities of those elements that pose a potential or actual threat to US and multinational forces.
4648 MSO are also employed to develop local source or informant networks providing early warning of
4649 imminent danger to US and multinational forces and contribute to mission planning.

4650 7-18. Formal contacts are individuals who have agreed to meet and cooperate with HUMINT collectors for
4651 the purpose of providing information. HUMINT collectors who have met with a particular continuous
4652 contact three or more times should consider assessing the contact for use as a formal contact. Formal
4653 contacts can be tasked, trained, and paid. Formal contacts meet repeatedly with HUMINT collectors, and
4654 their operation and tasking must be carried out in accordance with FM 2-22.3. Formal contacts are
4655 employed to develop HUMINT sources who can provide early warning of imminent danger to US and
4656 multinational forces and contribute to mission planning.

4657 7-19. HCTs must be able to travel to meet sources and be able to remain at a meeting location for long
4658 enough to conduct their meeting. This requirement to remain in one location for up to several hours means
4659 that HUMINT teams require dedicated security. Placing an HCT with a combat patrol for movement will

FOR OFFICIAL USE ONLY

4660 not serve to provide them with the support they need for stationary operations since combat patrols need to
4661 keep on the move.

4662 **LIAISON OPERATIONS**

4663 7-20. Liaison with local military, government, or civilian agency officials provides an
4664 opportunity to collect information required by the commander. The HUMINT collector meets
4665 with these officials to conduct liaison, coordinate certain operations, collect information, and
4666 obtain leads to potential sources of information. Elicitation is the primary technique used
4667 with liaison contacts, although in many cases there is a more formal exchange of
4668 information. Information obtained by these elements through liaison normally tends to
4669 reflect the official positions of their superiors and may not be entirely accurate or complete.

4670 **SUPPORT TO DOMEX, SITE EXPLOITATION, AND CAPTURED ENEMY EQUIPMENT**
4671 **EXPLOITATION OPERATIONS**

4672 7-21. The execution of DOMEX, site exploitation, and CEE exploitation operations is not exclusively a
4673 HUMINT function but may be conducted by any intelligence personnel with appropriate language support.
4674 Of particular interest to HUMINT collectors are CEDs. A CED is any document that has been in
4675 possession of the enemy, whether or not the enemy has created it for their use. HUMINT collectors can
4676 very effectively use CEDs to further exploit information of intelligence value during the conduct of
4677 operations.

4678 **CAPABILITIES AND PLANNING CONSIDERATIONS**

4679 7-22. The fundamentals of HUMINT include capabilities and planning considerations as discussed below.

4680 **CAPABILITIES**

4681 7-23. HUMINT collection capabilities include the ability to—

- 4682 ● Collect information and cross-cue from an almost endless variety of potential sources including
4683 friendly forces, civilians, detainees, and source-related documents.
- 4684 ● Focus on the collection of detailed information not available by other means. This includes
4685 information on threat intentions and local civilian and threat force attitudes and morale. It also
4686 includes building interiors and facilities that cannot be collected on by other means due to
4687 restrictive terrain.
- 4688 ● Corroborate or refute information collected from other reconnaissance and surveillance (R&S)
4689 assets.
- 4690 ● Operate with minimal equipment and deploy in all operational environments in support of
4691 offensive, defensive, stability and reconstruction operations, or civil support operations. Based
4692 on solid planning and preparation, HUMINT collection can provide timely information if
4693 deployed forward in support of maneuver elements.

4694 **PLANNING CONSIDERATIONS**

4695 7-24. The following are important considerations when conducting planning for HUMINT operations.

- 4696 ● **Interpersonal skills.** HUMINT is dependent on the subjective interpersonal capabilities of the
4697 individual rather than on the abilities to operate collection equipment. HUMINT collection
4698 capability is based on experience within a specific AO that can only be developed over time.
- 4699 ● **Availability of trained and certified personnel.** There are never enough HUMINT collectors
4700 to meet all requirements. Limited assets must be prioritized in support of units and operations
4701 based on their criticality.

FOR OFFICIAL USE ONLY

- 4702 ● **Time.** HUMINT collection, particularly source operations, takes time to develop. Collection
4703 requirements must be developed with sufficient lead time for collection.
- 4704 ● **HUMINT language limitations.** While HUMINT collectors can normally use an interpreter, a
4705 lack of language proficiency by the collector can significantly slow collection efforts. Such
4706 language proficiency takes time to develop.
- 4707 ● **Misuse of HUMINT personnel.** HUMINT collectors are frequently utilized incorrectly and
4708 assigned missions that belong to CA, MP, CI, interpreters, translators, or other operational
4709 specialties for which they are not trained or certified to conduct or supervise. Employing
4710 HUMINT collectors in any capacity other than HUMINT collection missions severely impacts
4711 their ability to answer intelligence requirements.
- 4712 ● **HUMINT collection capability.** HUMINT collection capability is limited when commanders
4713 do not provide support specifically to the HCT for the conduct of HUMINT collection missions.
4714 Often HCTs are required to travel with patrols in order to have mobility within the AO. While
4715 this does get the HCT off the base or camp, it does not allow them the time or flexibility to
4716 conduct a HUMINT collection mission. The nature of patrol missions requires them to keep on
4717 the move most of the time. HUMINT collection missions often require the HCT to remain at
4718 location for extended periods. In order for HUMINT collection missions to be successful,
4719 commanders must provide dedicated mission support to allow for this requirement.
- 4720 ● **HUMINT risk management.** Maneuver commanders, in weighing the risks associated with
4721 employing HCTs, should consider the potential loss of a wealth of information such as enemy
4722 activities, locations of high-value personnel, and threats to the force that they may incur if they
4723 restrict HCT collection activities.
- 4724 ● **HUMINT legal obligations.** Applicable US law and regulations and international law govern
4725 HUMINT collection operations. HUMINT operations may be further restricted by SOFAs and
4726 other agreements, execution orders, ROE, and local laws. Such documents, however, cannot
4727 permit interrogation actions which are illegal under US or international law.
- 4728 ● **HUMINT connectivity and bandwidth requirements.** With the exception of the SALUTE
4729 report, most HUMINT reporting requires considerable bandwidth. Deployed HCTs must be able
4730 to travel to and report from all areas in the AO. Digital communication equipment must be able
4731 to provide reliable connectivity with team reporting channels and sufficient bandwidth for
4732 transmission of reports, including digital imagery.
- 4733 ● **HUMINT reporting and immediate access to sources.** Except in tactical situations when
4734 HUMINT collectors are in immediate support of maneuver units, HUMINT collection and
4735 reporting takes time. In stability operations, sources need to be assessed and developed. Once
4736 they are developed, they need to be contacted which often takes time and coordination. In
4737 offensive and defensive operations, HUMINT collection at EPW holding areas sometimes may
4738 still be timely enough to meet tactical and operational requirements.

4739 HUMAN INTELLIGENCE ORGANIZATIONS

- 4740 7-25. Brigade Combat Team (BCT). The BCT's organic MI Company's Ground Collection Platoon has
4741 one four-person HUMINT OMT (consisting of a WO (351M), a HUMINT NCO (35M) and two junior
4742 enlisted Soldiers (35M) and three organic four-person HCTs (consisting of one E6 35M3L, one E5
4743 35M2L, one E4 35M10, and one E3 35M10). The HUMINT OMT provides the first level of technical
4744 channels, as well as management to subordinate HCTs that conduct HUMINT operations. The OMT must
4745 be prepared to control any additional HCT that may be pushed down from higher echelon to support the
4746 BCT.
- 4747 7-26. Stryker Brigade Combat Team (SBCT). The SBCT's organic MI Company's CI and HUMINT
4748 Collection Platoon has two organic HUMINT OMTs and four organic HUMINT teams, each with an
4749 organic CI agent. Additional HCTs (and OMTs) may be pushed down to the SBCT from the Division MI

FOR OFFICIAL USE ONLY

4750 Battalion. Within the SBCT Reconnaissance Squadron there is a total of 36 HUMINT collectors (35M)
4751 organic (12 per Reconnaissance Troop, four per Platoon, one per Squad.)

4752 7-27. Division. Within a Division the Battlefield Surveillance Brigade (BFSB) MI Battalion has three
4753 companies with HUMINT assets, and a HUMINT and CI team organic to the BFSB S-2. The C&E
4754 company has three HUMINT OMTs that control a total of 12 HCTs. The C&E company provides general
4755 support coverage for the division. The two CI/HUMINT companies each has four organic HUMINT OMTs
4756 that each controls a total of 16 HCTs. The CI/HUMINT company provides DS to the BCT. When HCTs
4757 are pushed down to SBCT or BCT level, OMTs may also be required to be pushed down to control the
4758 additional HUMINT assets.

4759 7-28. Theater. At Theater or JTF level, the INSCOM Military Intelligence Brigade has HUMINT assets
4760 that could be employed as HUMINT OMTs and HCTs to provide coverage for the supported unit or that
4761 could be pushed down to subordinate units.

4762 7-29. ASCC. HUMINT operations to satisfy Army-level intelligence requirements are satisfied by
4763 INSCOM's Army Operational Activity. The Army Operational activity also has the capability to provide
4764 HUMINT subject matter expert support to deployed commanders.

4765 **HUMAN INTELLIGENCE AUTHORITIES**

4766 7-30. The Secretary of Defense (SECDEF) has designated the Director of DIA as the Defense HUMINT
4767 Manager for the entire DOD. To assist the Defense HUMINT manager, a new organization called the
4768 Defense HUMINT Management Office has been established to provide standardization across DOD for
4769 HUMINT policy, training, and operations.

4770 7-31. The Undersecretary of Defense for Intelligence has promulgated new policy for the conduct of DOD
4771 HUMINT. The new policy designates the CCDRs, the Director of DIA, and the military service senior
4772 intelligence officers (Headquarters, Department of the Army [HQDA] DCS, G-2) as HUMINT executors.
4773 The SECDEF has given the HUMINT executors authority to approve their respective component's
4774 HUMINT activities in support of military operations. This means that the Army DCS G-2, can approve
4775 HUMINT activities conducted by the US Army in support of departmental or CCDR requirements.

4776 **HUMAN INTELLIGENCE TECHNICAL CHANNELS**

4777 7-32. HUMINT falls under the appropriate echelon 2X. See chapter 6 for details about 2X operations.
4778
4779
4780

FOR OFFICIAL USE ONLY

4781

Chapter 8

4782

Geospatial Intelligence

4783

INTRODUCTION

4784

8-1. There are many producers of GEOINT, and the users of GEOINT extend from the national level down to the lowest tactical level. The overall GEOINT enterprise that supports operations extends across all Services, multinational partners, and other organizations during joint operations and unified action. GEOINT requirements, methods of collection (and associated systems), and products vary widely based on the echelon of support and the various types of operations.

4785

4786

4787

4788

4789

8-2. The Army does not conduct GEOINT operations in isolation. GEOINT is comprised of many ongoing operations and activities across DOD. The NSG manages operations through guidance, policy, programs, and organizations. The NSG is the combination of technology, policies, capabilities, doctrine, activities, people, data, and communities necessary to produce GEOINT in the form of integrated intelligence across multiple environments. The NSG community consists of members and partners:

4790

4791

4792

4793

4794

- Members include the intelligence community, joint staff, military departments (to include the Services), and combatant commands.

4795

4796

4797

- Partners include civil applications committee members, international partners, industry, academia, defense service providers, and civil community service providers.

4798

NATIONAL SYSTEM FOR GEOSPATIAL-INTELLIGENCE AND

4799

NATIONAL GEOSPATIAL-INTELLIGENCE AGENCY

4800

8-3. The Director of NGA serves as the functional manager for GEOINT in accordance with applicable laws, DNI and DOD directives, guidance, and agreements. In that role, Director, NGA, also informs and guides NSG activities on GEOINT operations. Additionally, the NSG functional manager is responsible for the “end-to-end GEOINT process”; sets standards for the GEOINT architecture and products; and provides technical guidance for systems using GEOINT.

4801

4802

4803

4804

4805

8-4. Title 10 US Code § 467 establishes GEOINT. GEOINT is *the exploitation and analysis of imagery and geospatial information to describe, assess, and visually depict physical features and geographically referenced activities on the Earth. GEOINT consists of imagery, imagery intelligence, and geospatial information* (NGA Publication 1).

4806

4807

4808

4809

- **Imagery:** A likeness or representation of any natural or manmade feature or related object or activity and the positional data acquired at the same time the likeness or representation was acquired, including products produced by space-based national intelligence reconnaissance systems, and likenesses and representations produced by satellites, airborne platforms, unmanned aircraft systems (UASs), or similar means. This does not include handheld or clandestine photography taken by or on the behalf of HUMINT collection organization.

4810

4811

4812

4813

4814

4815

- **Imagery Intelligence:** The technical, geographic, and intelligence information derived through the interpretation or analysis of imagery and collateral materials.

4816

4817

- **Geospatial Information:** Information that identifies the geographic location and characteristics of natural or constructed features and boundaries on the Earth, including statistical data and information derived from, among other things, remote sensing, mapping and surveying technologies, and mapping, charting, geodetic data, and related products.

4818

4819

4820

FOR OFFICIAL USE ONLY

4821 8-5. The NGA as the functional manager published NSG Publication 1, the capstone GEOINT doctrine
4822 publication, in September 2006. This NSG doctrine explains that GEOINT is an intelligence discipline that
4823 has evolved from the integration of imagery, IMINT, and geospatial information. The basic capabilities and
4824 products of these three areas still exist as the foundation of GEOINT.

4825 8-6. NSG doctrine discusses four fundamental aspects of GEOINT:

- 4826 ● The discipline of GEOINT.
- 4827 ● The data that comprise GEOINT.
- 4828 ● The process used to develop GEOINT products.
- 4829 ● The products derived from GEOINT data.

4830 8-7. GEOINT provides a common framework for supporting joint operations to better enable mission
4831 accomplishments across the range of military operations and with all mission partners. GEOINT support to
4832 joint operations supports the multidirectional flow and integration of geospatially referenced data from all
4833 sources to achieve shared situational awareness of the operational environment, NRT tracking, and
4834 collaboration between forces. The GEOINT cell at the combatant command coordinates closely with the
4835 JFC GEOINT cell (if the combatant command and JFC are two different organizations) to ensure
4836 continuity in operations across all functions, organization levels, and levels of warfare.

4837 8-8. GEOINT activities necessary to support joint operations include capability to define GEOINT
4838 requirements; discover and obtain GEOINT; put GEOINT in a useable form; and then maintain, use, and
4839 share GEOINT. The GEOINT cell interfaces directly with the user to define user requirements and then
4840 interfaces with the NSG to obtain and provide the best quality GEOINT possible directly to the warfighter
4841 in fulfillment of the broad range of requirements depicted by the various mission functions. The GEOINT
4842 cell supports joint operations with five activities:

- 4843 ● Define GEOINT mission requirements.
- 4844 ● Obtain mission-essential GEOINT.
- 4845 ● Evaluate available GEOINT data.
- 4846 ● Use and disseminate GEOINT.
- 4847 ● Maintain and evaluate GEOINT.

4848 8-9. The use of GEOINT can be categorized into five general areas:

- 4849 ● GMI and I&W.
- 4850 ● Safety of navigation.
- 4851 ● Operational environmental awareness.
- 4852 ● Mission planning and C2.
- 4853 ● Target intelligence.

4854 8-10. The combatant commands develop area and point target GEOINT requirements to support the
4855 planning and execution of joint operations. The GEOINT cell assigned to combatant commands is
4856 responsible for coordinating all GEOINT requirements within its AOR while ensuring that the supporting
4857 commands or component commands are executing theater and mission-specific GEOINT requirements.
4858 This includes planning provisions for war reserve requirements and enabling the COP with a GEOINT
4859 framework for all needed layers of geospatial information.

4860 8-11. Each combatant command (except the US Strategic Command) has also established a JIOC to plan,
4861 prepare, integrate, direct, synchronize, and manage continuous full-spectrum defense intelligence
4862 operations. The goal of all JIOCs is the integration of intelligence into operations in order to increase the
4863 speed, power, and effectiveness of DOD operations. These organizations facilitate access to all available
4864 intelligence sources and analyze, produce, and disseminate timely, relevant, accurate, predictive, and
4865 tailored all-source intelligence and GEOINT to support planning and execution of military operations. The
4866 combatant commands have imagery exploitation capabilities and geospatial information and services
4867 capabilities.

FOR OFFICIAL USE ONLY

4868 8-12. The types of imagery-derived products generated by the combatant commands include text reports,
 4869 database entries, target materials and support products, visualization products, and annotated graphics. The
 4870 GEOINT cell provides advice to the CCDR on all geospatial information and geodetic sciences. While the
 4871 combatant commands rely heavily on basic maps, charts, target coordinates, geodetic surveys, and other
 4872 standard geospatial information provided by NGA, they also research, develop, and produce their own
 4873 mission-specific, specialized geospatial products and services for the CCDR and components. These
 4874 products (for example, aeronautical and hydrographic products, terrain graphics and data, charts,
 4875 perspective views, image graphics, target materials) provide value-added improvements to NGA digital
 4876 products.

4877 8-13. The NGA support team (NST) is the primary mechanism for interaction between the combatant
 4878 commands and NGA. The NST coordinates NGA's operational, policy, and training support to its
 4879 customers. NGA maintains NSTs at the Joint Staff, combatant commands, Services, and DOD agencies.

4880 8-14. A typical NST is composed of a senior representative (a military O-6 or a defense intelligence senior
 4881 leader), staff officers, and imagery and geospatial analysts. A reach component at NGA HQ focuses NGA
 4882 production support. In addition to using NSTs, NGA may deploy crisis or geospatial support teams of
 4883 imagery and geospatial analysts upon request, either independently, as augmentation to an existing NST, or
 4884 as part of a NIST. A NIST is a nationally sourced team composed of intelligence and communications
 4885 experts from DIA, CIA, National Security Agency (NSA), or any combination of these agencies.

4886 8-15. A NIST is a nationally sourced team composed of intelligence and communications experts from
 4887 DIA, CIA, NSA, or any combination of these agencies. These teams of government and/or contract
 4888 personnel employ deployable GEOINT production systems. NST personnel have reachback to NGA for
 4889 data and products, fuse this information with tactical and theater sources, and work with users to produce
 4890 products tailored to their needs. For more information on joint GEOINT doctrine, refer to JP 2-03.

4891 **GEOSPATIAL INTELLIGENCE WITHIN ARMY DOCTRINE**

4892 8-16. Based on the Army's organizational construct, GEOINT is described as intelligence derived from the
 4893 exploitation and analysis of imagery with geospatial information to describe, assess, and visually depict
 4894 physical features and geographically referenced activities in the operational environment. GEOINT
 4895 consists of imagery, IMINT, and geospatial information.

4896 8-17. There are unique characteristics of each Service's portion (or extension) of the GEOINT enterprise.
 4897 Each member of the enterprise has unique requirements. Within intelligence, the nature of a Service's
 4898 requirements drives the conduct of unique intelligence operations (tasking, collection, processing,
 4899 exploitation, dissemination, and the ultimate presentation).

4900 8-18. Army GEOINT operations are complementary to NGA and joint operations, and the Army works
 4901 within the same enterprise (the NSG) to improve the quality of intelligence support to all operations. Both
 4902 the Army Intelligence and Engineer communities recognize the DOD GEOINT enterprise—and everything
 4903 encompassed in the enterprise—and acknowledge GEOINT as an intelligence discipline. However, the
 4904 Army doctrinal distinction is based on the operational construct of an intelligence discipline that is
 4905 intelligence-product oriented. The full power of GEOINT for the Army is achieved from the integration
 4906 and analysis of all three capabilities, which results in more comprehensive and tailored intelligence
 4907 products for a wide scope of Army requirements and users across all of the warfighting functions.

4908 8-19. The Army implements GEOINT through both Engineer and MI units. Previously, Engineer and MI
 4909 units worked independently in the creation of GEOINT products. Currently, permanent Geospatial
 4910 Planning Cells (GPCs) are situated at the Army Service Component Command (ASCC); and the creation of
 4911 GEOINT Cells from the Brigade Combat Teams (BCT) to the ASCC provide for fully fused GEOINT
 4912 analysis functions as an inherent capability of J-2/G-2/S-2. The primary GEOINT services each brings to
 4913 the GEOINT cells are—

- 4914 ● MI units and organizations provide imagery and IMINT to the enterprise.

FOR OFFICIAL USE ONLY

4915 ● Engineer (topographic) units and organizations provide geospatial data and information to the
4916 enterprise.

4917 8-20. Geospatial engineer units that are located at the ASCC level are the GPCs. The GPC's mission is to
4918 collect, create, manage, and disseminate geospatial data, information and products for their AOR. The GPC
4919 is responsible for providing the geospatial data, information, and products to geospatial engineering units
4920 for dissemination to Army Battle Command Systems (ABCS) and to coordinate the acquisition and
4921 production activities of geospatial engineering units operating within the GPC's AOR. The GPC also
4922 coordinates with NGA, host or allied nation geospatial support activities, and higher headquarters in order
4923 to create and maintain geospatial architecture from national to tactical levels.

4924 8-21. The conduct of operations depends on geospatial data and imagery. That geospatial data and imagery
4925 is the foundation for the COP, and it facilitates situational understanding for all of the warfighting
4926 functions. The COP is a critical tool to integrate all Army operations by providing a common view of
4927 operations and the operational environment. One of the primary data managers for the COP is the
4928 geospatial engineer (within the GEOINT cell) at every echelon. The GEOINT cell is responsible for
4929 creating and maintaining the GEOINT database of the COP. The GEOINT database establishes the
4930 geospatial data foundation for the GEOINT cell. These databases include enterprise databases such as
4931 Theater Geospatial Database (TGD) and Imagery Product Library (IPL).

4932 8-22. The GEOINT cell provides direct support to create GEOINT products. The GEOINT cell is
4933 responsible for coordinating GEOINT requirements within the AOR. The GEOINT cell provides the
4934 commander visualization of the battlespace and manages the geospatial and imagery foundations of the
4935 COP. GEOINT cells provide a collaborative environment for the geospatial engineer and imagery analyst
4936 to achieve maximum development of GEOINT products.

4937 8-23. A cell is a group of personnel with specific skills brought together to accomplish key functions.
4938 GEOINT cells are comprised of geospatial engineers and imagery analysts working together to provide
4939 commanders a more complete picture of the physical environment and infrastructure in his operational
4940 environment. The advantages of GEOINT cells include centralized GEOINT production, synchronization
4941 of effort, reduction of redundancy, and maximization of the imagery analyst and the geospatial engineer
4942 skills.

4943 8-24. There are other differences in the Army construct: The Army—

4944 ● Views the current categories of imagery, IMINT, and geospatial information as sufficient and
4945 more specific for Army purposes. GEOINT is unique and necessary to describe a value-added to
4946 intelligence operations through analysis and integration and/or combination of imagery, IMINT,
4947 and geospatial information.

4948 *Note.* According to NSG Publication 1-0, “Almost any type of GEOINT can be produced
4949 without using intelligence analysis”]

4950 ● Geospatial engineers are not the sole providers of geospatial data and information to the
4951 enterprise. All Soldiers and units provide this data; the geospatial engineers verify and manage
4952 this data for the Army. Geospatial engineers also produce data and GEOINT products, enhance
4953 existing data, reconcile data conflicts, and analyze and disseminate data.

4954 ● Maintains a tactical intelligence architecture and uses systems that are significantly different
4955 from the other aspects of the GEOINT enterprise. NGA develops GEOINT architecture and
4956 standards for the GEOINT enterprise. Army intelligence units and organizations do not control
4957 all the different forms of data (imagery and geospatial), the different systems, and the tactical C2
4958 network.

4959 ● Manages commander's requirements for information that falls across all of the Army's
4960 warfighting functions and differs from NGA requirements to support DOD.

FOR OFFICIAL USE ONLY

- 4961 ● Has a doctrinal information hierarchy established in FM 6-0 that builds from data to information
4962 to knowledge to understanding. In this hierarchy, intelligence (depending on the level of detail)
4963 can be resident anywhere from the information to the understanding levels.
- 4964 8-25. The Army recognizes, as stated in NSG Publication 1-0, that GEOINT's added value is based on the
4965 prerequisite for analysis and the integration and/or combination of all three elements which results in more
4966 comprehensive and tailored intelligence support. Also, just like NGA, Army doctrine recognizes four
4967 fundamental aspects of GEOINT:
- 4968 ● GEOINT as an intelligence discipline. The GEOINT discipline encompasses all intelligence
4969 tasks and intelligence activities involved in the planning, collection, processing, analysis,
4970 exploitation, and dissemination of GEOINT.
 - 4971 ● GEOINT as the product defined above.
 - 4972 ● Unique processes used to develop GEOINT.
 - 4973 ● Unique data that is used to develop GEOINT.
- 4974 8-26. The goal of Army GEOINT operations is to provide tailored products that serve as the foundation for
4975 the COP and facilitate the commander's gaining situational understanding. Just as it states in NSG
4976 GEOINT Basic Doctrine Publication 1-0, "Advances in technology and the use of geospatial data have
4977 created the ability to integrate and/or combine elements of any or all of the areas, along with other elements
4978 of information, resulting in many new, more sophisticated capabilities for producing products and
4979 conducting analysis. ... Advanced technology now provides the capability to use and combine geospatial
4980 data in different ways to create interactive/dynamic, customized visual products. It allows the analyst to
4981 quickly make more complex connections between different types of data and information than previously
4982 possible." GEOINT is a major step toward improving Army intelligence and intelligence operations
4983
4984
4985

FOR OFFICIAL USE ONLY

4986

Chapter 9

4987

Imagery Intelligence

4988

DEFINITION

4989

9-1. *IMINT is the technical, geographic, and intelligence information derived through the interpretation or analysis of imagery and collateral materials (JP 2-03).*

4990

4991

9-2. Imagery analysis is the science of converting information extracted from imagery into intelligence about activities, issues, objects, installations, and/or AOIs.

4992

4993

9-3. Imagery is a likeness or presentation of any natural or manmade feature or related object or activity, and the positional data acquired at the same time the likeness or representation was acquired, including products produced by space-based national intelligence reconnaissance systems; and likeness and presentations produced by satellites, airborne platforms, UASs, or other similar means (except that such term does not include handheld or clandestine photography taken by or on behalf of human intelligence collection organizations) (JP 2-03).

4994

4995

4996

4997

4998

4999

ROLE

5000

9-4. The role of IMINT is to assist the commanders in applying and protecting their combat power. Imagery often enhances the commander's situational understanding of the AO. Imagery assets, particularly MTI systems, are useful in cueing other ISR systems. Other than direct human observation, imagery is the only intelligence discipline that allows the commanders to see the AO in NRT as the mission progresses. In those cases where maps are not available, digital imagery in hardcopy or softcopy can be used as a substitute. Imagery can also be used to update maps or produce grid-referenced graphics. Detailed mission planning often requires imagery, to include three-dimensional stereo images, in order to provide the degree of resolution necessary to support such specialized planning. (See FM 2-22.501, when published, for more information on IMINT.)

5001

5002

5003

5004

5005

5006

5007

5008

5009

FUNDAMENTALS

5010

9-5. Some imagery assets are very responsive to the individual CCIRs. Some imagery systems can directly transmit imagery into the tactical operations center; examples include imagery from unmanned aircraft systems and the Joint Surveillance Target Attack Radar System and Airborne Reconnaissance Low (ARL). This direct downlink enables the G-2/S-2 to use the imagery as soon as possible instead of having to wait for finished imagery products. Anyone can look at an image but a trained imagery analyst is necessary to accurately assess the intelligence value of the imaged data.

5011

5012

5013

5014

5015

5016

9-6. Imagery-related equipment has undergone a reduction in size as well as a reduction in the time it takes to provide products, particularly softcopy imagery. The modularity and size reduction of imagery analysis, processing, and display systems makes transport easier; this allows commanders to deploy with fewer systems than in the past and still retain those capabilities and systems (or subsystems) required to complete the mission. Imagery and imagery considerations include bandwidth, classification, releasability, and necessary equipment and software for imagery analysts to perform their mission. Additionally, data compression allows faster transmission of imagery products directly to the warfighter.

5017

5018

5019

5020

5021

5022

FOR OFFICIAL USE ONLY

5023 **SOURCES OF IMAGERY**

5024 9-7. There are two general sources of imagery: national technical means and commercial that includes
5025 satellite and airborne platforms. National imagery traditionally refers to imagery collected by DOD
5026 imagery systems. However, there are other sources of imagery provided by non-national sources such as
5027 the shuttle radar topography mission and commercial remote sensing efforts.

5028 **NATIONAL TECHNICAL MEANS**

5029 9-8. National systems are developed specifically for supporting the President of the United States, the
5030 SECDEF, other national agencies, and US military forces. These systems respond to the needs of the nation
5031 and those of the combatant commands.

5032 **COMMERCIAL**

5033 9-9. Commercial companies build, launch, and operate satellite and airborne imagery systems for profit.
5034 In times of crises, license agreements with the US Government obligate US commercial satellite imaging
5035 systems to provide data only to the US Government at the market value. This protects information
5036 concerning US operations from threat exploitation from commercial systems such as the Google Earth.
5037 However, the US Government could never afford to buy all the commercial imagery available for a crisis
5038 and foreign commercial imagery systems are not bound to this arrangement, so these imagery sources may
5039 be used by our nation's enemies and adversaries. Commercial imagery has become increasingly valuable
5040 for many reasons:

- 5041 ● Due to its unclassified nature, civil and commercial imagery is useful in an open environment,
5042 may be released to other government agencies, intergovernmental organizations, NGOs, and
5043 multinational partners, and can be made available for public release.
- 5044 ● The use of civil and commercial imagery allows national technical means systems more time to
5045 focus on other intelligence functions.
- 5046 ● Civil and commercial imagery sources and companies offer electro-optical and radar imagery.
5047 Some offer large area collection useful for broad area coverage purposes.

5048 9-10. The National Geospatial-Intelligence Agency's Source is responsible for ordering commercial
5049 imagery. The Commercial Satellite Imagery Library and the Unclassified National Imagery Library are
5050 available to research DOD-purchased commercial imagery. The G-2/S-2 should consult the NGA Source
5051 when forming commercial imagery requests. NGA will deliver the imagery primarily on CD-ROM media
5052 via courier or mail service. Limited digital or electronic delivery is available as well.

5053 **TYPES OF IMAGERY SENSORS**

5054 9-11. There are two general types of imagery sensors: electro-optical and radar. Electro-optical sensors
5055 include panchromatic (visible), infrared, spectral (multispectral and hyperspectral), polarimetric, and light
5056 detection and ranging. Radar sensors are synthetic aperture radar systems. These systems collect and
5057 display data as either fixed target indicators or moving target indicators. Each sensor and platform has a
5058 unique capability, with distinct advantages and disadvantages. The G-2/S-2 must understand each sensor's
5059 and platform's capability in order to select the best for the mission and thus enable the user to better
5060 understand the intelligence received. Certain sensors are better suited for military operations than others.
5061 Table 9-1 lists sensor capabilities.

FOR OFFICIAL USE ONLY

5062

Table 9-1. Sensor characteristics matrix

SENSORS	ADVANTAGES	DISADVANTAGES
Panchromatic (Visible) Best tool for daytime, clear weather, detailed analysis. Includes video and electro-optical.	<ul style="list-style-type: none"> • Affords a familiar view of a scene. • Offers system resolution that cannot be achieved in other optical systems or in thermal images and radars. • Preferred for detailed analysis and mensuration. • Offers stereoscopic viewing. 	<ul style="list-style-type: none"> • Restricted by terrain and vegetation. • Limited to daytime use only. • Reduced picture size. • Degraded imagery in other than clear weather.
Infrared Best tool for nighttime, clear weather, detailed analysis. Includes Overhead Non-Imaging Infrared.	<ul style="list-style-type: none"> • A passive sensor and is impossible to jam. • Offers camouflage penetration. • Provides good resolution. • Nighttime imaging capability. 	<ul style="list-style-type: none"> • Not effective during thermal crossover periods. • Product not easily interpretable. • Requires skilled analysis. • Cannot penetrate clouds.
Radar Useful for detecting presence of objects at night and in bad weather. Includes synthetic aperture radar, coherent change detection, and MTI.	<ul style="list-style-type: none"> • All weather; can penetrate fog, haze, clouds, smoke. • Day or night use. • Does not rely on visible light nor thermal radiation. • Good standoff capability. • Large area coverage. • Allows moving target detection. • Foliage and ground penetration. 	<ul style="list-style-type: none"> • Product not easily interpretable. • Requires skilled analysis. • Terrain masking inhibits use.
Multispectral Imagery Best tool for mapping purposes and terrain analysis.	<ul style="list-style-type: none"> • Large database available. • Band combinations can be manipulated to display desired requirements. • Images can be merged with other digital data to provide higher resolution. 	<ul style="list-style-type: none"> • Product not easily interpretable. • Requires skilled analysis. • Computer manipulation requires large amounts of memory and storage; requires large processing capabilities.

5063 **IMAGERY INTELLIGENCE IN THE INTELLIGENCE PROCESS**

5064 9-12. The IMINT discipline has several unique considerations throughout the steps of the intelligence
5065 process.

5066 **GENERATE INTELLIGENCE KNOWLEDGE**

5067 9-13. The G-2/S-2 should research targets using online imagery databases early and request those imagery
5068 products that are not perishable for contingency planning. National and combatant command imagery
5069 databases may hold recently imaged areas that could meet the commander's immediate needs instead of
5070 requesting new imagery.

FOR OFFICIAL USE ONLY

5071 **PLAN**

5072 9-14. The first step in planning for IMINT is determining the need for IMINT products based on the PIRs
5073 and the initial IPB. The staff must clearly articulate their intelligence requirements to include
5074 communicating what the mission is and how the requested product will aid in mission accomplishment.
5075 The G-2/S-2 should submit the imagery exploitation and collection requirements in the Requirements
5076 Management System using established procedures such as those in the unit's SOP or as established by the
5077 combatant command.

5078 9-15. The G-2/S-2 must also determine the specific imagery requirements to avoid burdening the system
5079 with unnecessary requests. The desire for imagery products often exceeds the capabilities of the imaging
5080 system. Therefore, it is imperative that the G-2/S-2 consider what type of analysis is needed and request
5081 only that which they require. The specifications of the request for IMINT products often affect the
5082 timeliness of the response. For example, determining if vehicles are tanks takes less time and requires less
5083 resolution than determining the make, model, and capabilities of the tank.

5084 9-16. IMINT products to be considered for requirements by the G-2/S-2 include—

- 5085 ● Imagery to detect and/or identify and locate, for example, specific unit types, equipment,
5086 obstacles, and potential field fortifications from which intelligence analysts are able to analyze
5087 enemy capabilities and develop possible COAs.
- 5088 ● Imagery to update maps and enhance the interpretation of information from maps. Detailed
5089 mission planning uses imagery to include stereo images for three-dimensional viewing of the
5090 terrain and many other geospatial uses.
- 5091 ● Moving target indicator (MTI) and full-motion video displays or products that provide an NRT
5092 picture of an object's movement by indicating its speed, location, and direction of travel. MTI
5093 systems do not differentiate friendly from enemy.
- 5094 ● Imagery to support protection of the force by helping commanders visualize how their forces
5095 look—including their disposition, composition, and vulnerabilities—as exploited by enemy
5096 IMINT systems.
- 5097 ● Target packets with imagery of the HVTs or HVIs and HPTs that include the critical elements of
5098 the targets and potential collateral damage.
- 5099 ● Imagery to support combat assessment to confirm destruction, determine the percentage of
5100 destruction, or whether the target was unaffected.
- 5101 ● Advanced geospatial intelligence products that can determine change detection, specific weapon
5102 system identifications, chemical compositions and material content, and a threat's ability to
5103 employ these weapons.

5104 **PREPARE**

5105 9-17. The G-2/S-2 IMINT-related actions during the prepare step of the intelligence process include
5106 establishing or verifying the portion of the intelligence communications architecture that supports IMINT
5107 display and analysis functions properly. Additionally, the G-2/S-2 must ensure that required IMINT
5108 analytical assets and resources are prepared to provide support or are available through intelligence reach.
5109 Lastly, the G-2/S-2 must also ensure IMINT reporting and dissemination channels and procedures are in
5110 place and rehearsals are conducted with all pertinent IMINT elements to ensure interoperability.

5111 **COLLECT**

5112 9-18. As previously mentioned, there are two general types of imagery sensors. Depending on the type, the
5113 sensor or platform can record hardcopy or softcopy still (single frame) imagery or motion imagery. A given
5114 target will not necessarily receive continuous coverage due to the possible conflict between the number and
5115 priority of targets and the number and availability of imaging assets. However, a commander may decide to
5116 have continuous surveillance of certain targets, for specified periods, usually using organic imaging assets

FOR OFFICIAL USE ONLY

5117 (for example, unmanned aircraft systems) even though this detracts from the commander's ability to use
5118 these assets for other imagery targets within the AOI.

5119 9-19. Processing IMINT involves converting geospatial data into an image format that is suitable for
5120 performing analysis and producing intelligence. Examples of imagery processing include developing film,
5121 enhancing imagery, converting electronic data into visual displays or graphics, and constructing electronic
5122 images from geospatial data.

5123 **PRODUCE**

5124 9-20. The imagery analyst must ensure the IMINT product satisfies the associated intelligence
5125 requirements and that the product is in the required format. The quality and resolution of the product is
5126 highly dependent upon the type of sensor, the platform, the time of day, and the weather conditions, as well
5127 as the imagery analyst's ability to identify objects and analyze activity within the images.

5128 **ANALYZE**

5129 9-21. Timeliness is critical not only to imagery collection but also to imagery analysis and reporting. It is
5130 difficult to separate IMINT reporting from imagery analysis in this discussion; this is demonstrated by the
5131 three phases of IMINT reporting presented below; all are dependent upon the timeliness requirements.
5132 Each phase represents a different degree of analysis and period available to accomplish the exploitation of
5133 the imagery.

- 5134 • **First Phase** imagery analysis is the rapid exploitation of newly acquired imagery and reporting
5135 of imagery-derived information within a specified time from receipt of imagery. This phase
5136 satisfies PIRs and/or identifies changes or activity of immediate significance. First phase
5137 imagery analysis results in an Initial Phase Imagery Report and is usually completed within 45
5138 minutes after receipt of the imagery.
- 5139 • **Second Phase** imagery analysis is the detailed exploitation of newly acquired imagery and the
5140 reporting of imagery-derived intelligence and information while meeting the production and
5141 timeliness requirements. Other intelligence discipline source material may support Second phase
5142 imagery as appropriate. Second phase imagery analysis results in a Supplemental Imagery
5143 Report.
- 5144 • **Third Phase** imagery analysis is the detailed analysis of all available imagery pertinent to a SIR
5145 and the subsequent production and reporting resulting from this analysis within a specified time.
5146 This phase provides an organized detailed analysis of an imagery target or topic, using imagery
5147 as the primary data source but incorporating data from other sources as appropriate.

5148 9-22. The two types of imagery exploitation are national and direct support.

- 5149 • **National exploitation** is imagery exploitation that supports presidential requirements, National
5150 Security Council requirements, congressional requirements, or requirements of a common
5151 concern to the intelligence community.
- 5152 • **Direct support exploitation** is imagery exploitation that supports assigned missions of a single
5153 agency, department, or command.

5154 9-23. Imagery analysts will complete DS exploitation in order to satisfy (First Phase) requirements and
5155 report the results as soon as possible. Timelines for completing first phase exploitation varies depending on
5156 unit SOPs; however, the most commonly accepted timeline is to have the exploitation completed within
5157 four hours after receipt of the imagery. Collectors will complete national exploitation in order to satisfy
5158 (Second and Third Phases) requirements and report the results within the time specifications of each
5159 individual requirement.

FOR OFFICIAL USE ONLY

5160 **ASSESS**

5161 9-24. The requestor should immediately assess the imagery product upon receipt for accuracy and
5162 relevance to the original request. The requestor must then notify and inform the imagery analyst of the
5163 extent to which the product answered the PIR. Providing feedback to the producer regarding the product
5164 helps ensure the producer will provide the required information in the correct format. The following are
5165 some of the questions which the requestor should consider when providing feedback to the producer.

- 5166 ● Is the format of the product acceptable?
- 5167 ● Is additional information needed on the product or future products?
- 5168 ● Is excess information included on the product?
- 5169 ● Does the IMINT product satisfy the requirement?

5170 **PROPAGATE**

5171 9-25. IMINT products are propagated in hardcopy and digital formats. The distribution of hardcopy
5172 products will be via couriers or other types of mail systems. The requestor must ensure that the requested
5173 product is transmittable over the available communications systems.
5174

FINAL DRAFT

FOR OFFICIAL USE ONLY

5175

Chapter 10

5176

Measurement and Signature Intelligence

5177

DEFINITION

5178

10-1. MASINT is intelligence obtained by quantitative and qualitative analysis of data (metric, angle, spatial, wavelength, time dependence, modulation, plasma, and hydromagnetic) derived from specific technical sensors for the purpose of identifying any distinctive features associated with the emitter or sender, and to facilitate subsequent identification and/or measurement of the same. The detected feature may be either reflected or emitted (JP 2-0).

5179

5180

5181

5182

5183

10-2. MASINT collection systems include but are not limited to radar, spectroradiometric, electro-optical, acoustic, RF, nuclear detection, and seismic sensors, as well as techniques for collecting CBRNE and other materiel samples.

5184

5185

5186

10-3. It requires the translation of technical data into recognizable and useful target features and performance characteristics. Computer, communication, data, and display processing technologies now provide MASINT in support of commanders in full spectrum operations.

5187

5188

5189

10-4. There are six subdisciplines within MASINT:

5190

- **Radar.** The active or passive collection of energy reflected from a target or object by line of sight, bistatic, or over-the-horizon radar systems. Radar derived collection provides information on radar cross-sections, tracking, precise spatial measurements of components, motion and radar reflectance, and absorption characteristics for dynamic targets and objectives. A side-looking airborne radar system, coupled with advanced MASINT processing techniques—

5191

5192

5193

5194

- Provides a high resolution, day-and-night collection capability.
- Can produce a variety of intelligence products that identify or provide change detection, terrain mapping, underwater obstacles, dynamic sensing of targets in clutter, and radar cross-section signature measurements.

5195

5196

5197

5198

5199

- **RF.** The collection, processing, and exploitation of electromagnetic emissions from a RF weapon, an RF weapon precursor, or an RF weapon simulator; collateral signals from other weapons, weapon precursors, or weapon simulators (for example, electromagnetic pulse signals associated with nuclear bursts); and spurious or unintentional signals.

5200

5201

5202

5203

- **Electromagnetic Pulses.** Measurable bursts of energy that result from a rapid change in a material or medium, resulting in an explosive force, produces RF emissions. The RF pulse emissions associated with nuclear testing, advanced technology devices, power and propulsion systems, or other impulsive events can be used to detect, locate, identify, characterize, and target threats.

5204

5205

5206

5207

5208

- **Unintentional Radiation.** The integration and specialized application of MASINT techniques against unintentional radiation sources that are incidental to the RF propagation and operating characteristics of military and civil engines, power sources, weapons systems, electronic systems, machinery, equipment, or instruments. These techniques may be valuable in detecting, tracking, and monitoring a variety of activities of interest.

5209

5210

5211

5212

5213

- **Electro-Optical.** The collection, processing, exploitation, and analysis of emitted or reflected energy across the optical portion (ultraviolet, visible, and infrared) of the electromagnetic spectrum. MASINT electro-optical provides detailed information on the radiant intensities, dynamic motion, spectral and spatial characteristics, and the materials composition of a target.

5214

5215

5216

FOR OFFICIAL USE ONLY

- 5217 Electro-optical data collection has broad application to a variety of military, civil, economic, and
5218 environmental targets. Electro-optical sensor devices include radiometers, spectrometers, non-
5219 literal imaging systems, lasers, or laser detection and ranging systems.
- 5220 ■ **Infrared.** A subcategory of electro-optical that includes data collection across the infrared
5221 portion of the electromagnetic spectrum where spectral and thermal properties are
5222 measured.
 - 5223 ■ **LASER.** Integration and specialized application of MASINT electro-optical and other
5224 collection to gather data on laser systems. The focus of the collection is on laser detection,
5225 laser threat warning, and precise measurement of the frequencies, power levels, wave
5226 propagation, determination of power source, and other technical and operating
5227 characteristics associated with laser systems—strategic and tactical weapons, range finders,
5228 and illuminators.
 - 5229 ■ **Hyperspectral Imagery.** A subcategory of electro-optical intelligence produced from
5230 reflected or emitted energy in the visible and infrared spectrum used to improve target
5231 detection, discrimination, and recognition. Hyperspectral imagery can detect specific types
5232 of foliage (supporting drug-crop identification; disturbed soil); supporting the identification
5233 of mass graves, minefields, caches, underground facilities or cut foliage; and variances in
5234 soil, foliage, and hydrologic features—often supporting CBRNE contaminant detection.
 - 5235 ■ **Spectroradiometric Products.** Products that include electro-optical spectral (frequency) and
5236 radiometric (energy) measurements. A spectral plot represents radiant intensity versus
5237 wavelength at an instant in time. The number of spectral bands in a sensor system
5238 determines the amount of detail that can be obtained about the source of the object being
5239 viewed. Sensor systems range from multispectral (2 to 100 bands) to hyperspectral (100 to
5240 1,000 bands) to ultraspectral (1,000+ bands). More bands provide more discrete
5241 information, or greater resolution. The characteristic emission and absorption spectra serve
5242 to signature or define the makeup of the feature that was observed. A radiometric plot
5243 represents the radiant intensity versus time. An example is the radiant intensity plot of a
5244 missile exhaust plume as the missile is in flight. The intensity or brightness of the object is
5245 a function of several conditions including its temperature, surface properties or material,
5246 and how fast it is moving. For each point along a time-intensity radiometric plot, a spectral
5247 plot can be generated based on the number of spectral bands in the collector.
 - 5248 ● **Geophysical.** Geophysical MASINT involves phenomena transmitted through the earth
5249 (ground, water, atmosphere) and manmade structures including emitted or reflected sounds,
5250 pressure waves, vibrations, and magnetic field or ionosphere disturbances. Unattended ground
5251 sensors are an example of geophysical sensors.
 - 5252 ■ **Seismic.** The passive collection and measurement of seismic waves or vibrations in the
5253 earth surface.
 - 5254 ■ **Acoustic.** The collection of passive or active emitted or reflected sounds, pressure waves,
5255 or vibrations in the atmosphere or in the water. Water-based systems detect, identify, and
5256 track ships and submarines operating in the ocean.
 - 5257 ■ **Magnetic.** The collection of detectable magnetic field anomalies in the earth's magnetic
5258 field (land and sea). Magnetic sensors have the capability to indicate the presence and
5259 direction of travel of an iron object.
 - 5260 ● **Nuclear Radiation.** The information derived from nuclear radiation and other physical
5261 phenomena associated with nuclear weapons, reactors, processes, materials, devices, and
5262 facilities. Nuclear monitoring can be done remotely or during onsite inspections of nuclear
5263 facilities. Data exploitation results in characterization of nuclear weapons, reactors, and
5264 materials. A number of systems detect and monitor the world for nuclear explosions, as well as
5265 nuclear materials production.
 - 5266 ● **Materials.** The collection, processing, and analysis of gas, liquid, or solid samples. Materials
5267 intelligence is critical to collection against CBRNE warfare threats. It is also important to

FOR OFFICIAL USE ONLY

5268 analyzing military and civil manufacturing activities, public health concerns, and environmental
 5269 problems. Samples are both collected by automatic equipment, such as air samplers, and directly
 5270 by humans. Samples, once collected, may be rapidly characterized or undergo extensive forensic
 5271 laboratory analysis to determine the identity and characteristics of the sources of the samples.

5272 **ROLE**

5273 10-5. MASINT provides intelligence to the commander in full spectrum operations to facilitate situational
 5274 understanding. MASINT can defeat many of the camouflage, concealment, and deception techniques
 5275 currently used to deceive ISR systems.

5276 10-6. By application of NRT analysis and dissemination, MASINT has a potential ability to provide timely
 5277 situational awareness and targeting not necessarily available to other disciplines. Specifically, MASINT
 5278 sensors have unique capabilities to detect missile launch; detect and track aircraft, ships, and vehicles;
 5279 perform non-cooperative target identification and combat assessment; and detect and track fallout from
 5280 nuclear detonations. Often, these contributions are the first indicators of hostile activities.

5281 10-7. The MASINT systems most familiar on today's battlefield are employed by ground surveillance and
 5282 CBRN reconnaissance elements. MASINT spans the entire electromagnetic spectrum and its capabilities
 5283 complement, rather than compete with, the other intelligence disciplines. MASINT provides, to varying
 5284 degrees, the capability to—

- 5285 ● Use automatic target recognition and aided target recognition.
- 5286 ● Penetrate manmade and/or natural camouflage.
- 5287 ● Penetrate manmade and/or natural cover, including the ability to detect subterranean anomalies
 5288 or targets.
- 5289 ● Counter stealth technology.
- 5290 ● Detect recently placed mines.
- 5291 ● Detect natural or manmade environmental disturbances in the earth's surface not discernible
 5292 through other intelligence means.
- 5293 ● Provide signatures (target identification) to munitions and sensors.
- 5294 ● Enhance passive identification of friend or foe.
- 5295 ● Detect the presence of CBRNE agents to include prior to, during, or after employment.
- 5296 ● Detect signature anomalies that may affect target-sensing systems.

5297 **FUNDAMENTALS**

5298 10-8. Within DOD, there are two agencies that provide policy and guidance for MASINT. NGA is
 5299 responsible for the radar and electro-optical subdisciplines while DIA maintains the other four. While
 5300 NGA and DIA provide policy and guidance for MASINT, their policy and guidance remain transparent to
 5301 the service component. Each service, in turn, has a primary command or staff activity to develop
 5302 requirements and coordinate MASINT effort. The Army G-2 staff is the functional manager for Army
 5303 MASINT resources, policy, and guidance. Army weapons systems programs that require MASINT
 5304 information to support system design or operations submit requests through the Army Reprogramming
 5305 Analysis Team or INSCOM channels for data collection and processing.

5306 10-9. The S&TI community also performs MASINT collection and processing primarily to support R&D
 5307 programs and signature development. Every S&TI center has some involvement in MASINT collection or
 5308 production that reflects that center's overall mission (for example, NGIC has responsibility for armored
 5309 vehicles and artillery). Service R&D centers such as the Communications-Electronics Command Research,
 5310 Development, and Engineering Center, the Army Research Laboratory (ARL), and the Night Vision and
 5311 Electronic Systems Laboratory are also involved in developing sensor systems for collecting and
 5312 processing MASINT.

FOR OFFICIAL USE ONLY

5313 10-10. In addition to supporting the S&TI mission, INSCOM units also execute limited ground-based
5314 operational collection to support the ASCC and subordinate units. This capability will expand upon the
5315 standup of INSCOM MIBs.

5316 **MEASUREMENT AND SIGNATURE INTELLIGENCE IN THE**
5317 **INTELLIGENCE PROCESS**

5318 10-11. The MASINT discipline has several unique considerations throughout the steps of the intelligence
5319 process.

5320 **GENERATE INTELLIGENCE KNOWLEDGE**

5321 10-12. The G-2/S-2 section must research targets' characteristics and capabilities that may impact on the
5322 employment and use of MASINT sensors utilizing all available data prior to conducting operations.
5323 Additionally, the G-2/S-2 section must collect any existing MASINT products and identify all units,
5324 organizations, and systems that may potentially answer the commander's requirements. National and
5325 combatant command databases may hold more recent or updated information that can assist MASINT
5326 planners in determining the most effective MASINT means of supporting the commander's requirements.

5327 **PLAN**

5328 10-13. Some MASINT sensors can provide extremely specific information about detected targets,
5329 whereas other sensors may only be capable of providing an indication that an entity was detected.
5330 Additionally, there are varying capabilities of detection, identification, and classification among MASINT
5331 sensors. It is these varying capabilities that require synchronizing the employment of MASINT sensors
5332 both within the MASINT discipline and within the ISR effort as a whole. See FM 2-01 for more
5333 information on ISR synchronization.

5334 10-14. Depending on the type of sensor employed, a given MASINT collection target or NAI may not
5335 necessarily receive continuous coverage due to the possible conflict between the number and priority of
5336 targets and the number and availability of MASINT assets. However, a commander may decide to have
5337 continuous surveillance of certain targets by using available MASINT assets (for example, Unattended
5338 Ground Sensors (UGS) OmniSense, Silent Watch, and Scorpion).

5339 10-15. Another consideration when planning MASINT missions is whether to use active, passive, or a
5340 combination of sensors when planning MASINT coverage. This must be planned based on the
5341 commander's intent, the mission, the mission variables and the capabilities of the sensors. Additionally,
5342 personnel must be detailed to emplace the sensors (and retransmission systems, if necessary) and monitor
5343 the signatures that they transmit upon detection.

5344 **PREPARE**

5345 10-16. The primary responsibility of the G-2/S-2 during the prepare function of the intelligence process
5346 or MASINT is to support the G-3/S-3 in identifying the best locations to emplace MASINT assets and to
5347 ensure that the G-2/S-2 analysts can receive and verify the information transmitted by those assets.
5348 Additionally, the G-2/S-2 must ensure that required MASINT analytical assets and resources are prepared
5349 to provide support or are available through intelligence reach. Since the products of MASINT are not as
5350 well known as products from other intelligence disciplines, the G-2/S-2 must be aware of the types of
5351 MASINT products available to support the operation, and then educate the rest of his unit's staff on the use
5352 of these MASINT products. Lastly, the G-2/S-2 must also ensure MASINT reporting and dissemination
5353 channels and procedures are in place and rehearsals are conducted with all pertinent MASINT elements to
5354 ensure interoperability.

FOR OFFICIAL USE ONLY

5355 COLLECT

5356 10-17. MASINT provides information required to answer PIRs and other intelligence requirements in
 5357 support of the ISR effort. As stated earlier in this chapter, MASINT collection must not only be
 5358 synchronized within its own discipline but also be synchronized and integrated into the unit's overall ISR
 5359 effort in order to be effective. MASINT sensors are employed throughout the full spectrum of operations
 5360 from a variety of platforms—subsurface, ground, marine, and aerospace.

5361 10-18. Just as in the other intelligence disciplines, MASINT involves dealing with huge volumes of data
 5362 that have to be processed before beginning analysis and production. The process function regarding
 5363 MASINT involves converting esoteric data into a form that is suitable for performing analysis and
 5364 producing intelligence. MASINT processing can include relatively simple actions such as converting a
 5365 UGS sensor activation into a report, to a complex task such as processing hyperspectral imagery into a
 5366 report identifying the composition and concentrations of carcinogenic chemicals present in the emissions
 5367 from a factory upwind from a US forces encampment.

5368 PRODUCE

5369 10-19. Effective and timely MASINT requires personnel with diverse skill sets. The MASINT producer
 5370 must ensure the MASINT product satisfies the associated intelligence requirements and that the product is
 5371 in the required format. The quality, fidelity, and timeliness of MASINT products are highly dependent
 5372 upon the type of target, the collection system, the system's position in relation to the target or NAI, and the
 5373 weather, as well as the MASINT system operator's ability to identify the appropriate threat activity. The
 5374 objective of MASINT production is to be used in an all-source analytical approach.

5375 ANALYZE

5376 10-20. The intelligence staff analyzes intelligence and information about the enemy's equipment,
 5377 doctrine, and TTP. Using this information, along with the knowledge of friendly force MASINT
 5378 capabilities, the intelligence staff develops and refines a collection strategy to maximize the use of the
 5379 unit's MASINT systems to answer intelligence gaps.

5380 ASSESS

5381 10-21. The primary goal of the MASINT assess function is to determine whether the results of MASINT
 5382 collection and production meet the requirements of the unit's ISR effort. MASINT producers must assess
 5383 all facets of MASINT operations, from receipt of the ISR task to the dissemination of MASINT, in an
 5384 effort to determine the effectiveness of MASINT. An assessment of the friendly force's capabilities must
 5385 be conducted to ensure the continued effectiveness of, or to improve upon, MASINT collection. This
 5386 assessment is not only directed at each MASINT asset individually but also throughout the supporting
 5387 intelligence communications architecture, to include intelligence reach and the unit's entire ISR effort.

5388 10-22. Additionally, the G-2/S-2 immediately assesses MASINT products upon receipt for accuracy and
 5389 relevance. He must inform the MASINT producer of the extent to which the product answered the PIR or
 5390 intelligence requirement. Providing feedback to the MASINT producer—and collector—helps improve the
 5391 effectiveness and efficiency of MASINT.

5392 PROPAGATE

5393 10-23. MASINT of critical importance to the force, including answers to the PIRs, is disseminated via the
 5394 most expeditious means possible.

5395 10-24. For intelligence reach operations, MASINT products are available and disseminated in a variety of
 5396 forms. The requestor must ensure that the MASINT product can be transmitted over the available
 5397 communications systems, to include verifying the appropriate security level of the communications system.

FOR OFFICIAL USE ONLY

5398
5399

FINAL DRAFT

FOR OFFICIAL USE ONLY

5400

Chapter 11

5401

Open-Source Intelligence

5402

DEFINITION

5403

11-1. **Open-source intelligence** is *information of potential intelligence value that is available to the general public (JP 2-0)*. OSINT is derived from the systematic collection, processing, and analysis of publicly available, relevant information in response to intelligence requirements. Two important related terms are—

5404

5405

5406

5407

- **Open source**, which is any person or group that provides information without the expectation of privacy—the information, the relationship, or both is not protected against public disclosure.

5408

5409

- **Publicly available information**, which is data, facts, instructions, or other material published or broadcast for general public consumption; available on request to a member of the general public; lawfully seen or heard by any casual observer; or made available at a meeting open to the general public.

5410

5411

5412

5413

ROLE OF OPEN-SOURCE INTELLIGENCE

5414

11-2. OSINT operations are integral to Army intelligence operations. The availability, depth, and range of publicly available information enable intelligence organizations to satisfy many intelligence requirements without the use of specialized human or technical means of collection. OSINT operations support other ISR efforts by providing general initial information that supports generate intelligence knowledge and enhances collection and production. As part of a single-source and all-source intelligence effort, the use and integration of OSINT ensures commanders have the benefit of all available information. All OSINT operations conducted by intelligence personnel must be in compliance with the legal restrictions in Executive Order 12333, DOD Directive 5100.20, and AR 381-10.

5415

5416

5417

5418

5419

5420

5421

5422

11-3. The source, the information, and the collection means rather than a specific category of technical or human resources distinguish OSINT from other intelligence disciplines. Open sources broadcast, publish, or otherwise distribute unclassified information for public use. The collection means (techniques) for obtaining publicly available information from these media of communications are unintrusive. Other intelligence disciplines use confidential sources or intrusive techniques to collect private information. Confidential sources and private information are—

5423

5424

5425

5426

5427

- **Confidential source**, which is any person, group, or system that provides information with the expectation that the information, relationship, or both, are protected against public disclosure.
- **Private information**, which is data, facts, instructions, or other material intended for or restricted to a particular person, group, or organization. There are two subcategories of private information: classified information and controlled unclassified information.
 - **Classified information** requires protection against unauthorized disclosure and is marked to indicate its classified status when in documentary or readable form.
 - **Controlled unclassified information** requires the application of controls and protective measures, for a variety of reasons (that is, sensitive but unclassified, or for official use only), not to include those that qualify for formal classification.

5428

5429

5430

5431

5432

5433

5434

5435

5436

5437

FOR OFFICIAL USE ONLY

5438 11-4. The following characteristics address the role of publicly available information and OSINT in Army
5439 operations.

- 5440 ● **Provides the Foundation.** The US social structures, education system, news services, and
5441 entertainment industry shape our world view, awareness of international events, and perceptions
5442 of non-US societies. This foundation is an essential part of the generate intelligence knowledge
5443 step of the intelligence process.
- 5444 ● **Answers Requirements.** The availability, depth, and range of public information enable
5445 intelligence and non-intelligence organizations to satisfy many of the CCIRs (PIRs and FFIRs)
5446 and information requirements without the use of specialized human or technical means of
5447 collection. Given the volume, scope, and quality of publicly available information, OSINT
5448 operations can often proceed directly from the planning phase to the production phase of the
5449 intelligence process.
- 5450 ● **Enhances Collection.** Open-source research and collection support other surveillance and
5451 reconnaissance activities by answering requirements and providing foundational information
5452 (biographies, cultural information, geospatial information, technical data) that optimizes the
5453 employment and performance of sensitive human and technical means of collection.
- 5454 ● **Enhances Production.** As part of single-source and all-source intelligence production, the use
5455 and integration of OSINT ensures commanders have the benefit of all sources of available
5456 information.

5457 **FUNDAMENTALS OF OPEN-SOURCE INFORMATION**

5458 11-5. The Army does not have a specific MOS, additional skill identifier (ASI), or SQI for OSINT. With
5459 the exception of the Asian Studies Detachment, the Army does not have base TOE for OSINT units or staff
5460 elements. OSINT missions and tasks are imbedded within existing missions and force structure or
5461 accomplished through task organization.

5462 11-6. The focus of Army OSINT operations is the MIB. Each of these INSCOM units conducts sustained,
5463 regionally focused intelligence operations in support of their ASCC and combatant command. While their
5464 OSINT capabilities may vary, each of these theater-level MI units is the focal point within the combatant
5465 command for managing Army open-source requirements and providing OSINT support to Army tactical
5466 units deploying to or operating within the combatant command's AOR. When open-source skills and
5467 regional knowledge are not present in these deploying tactical units, personnel from the MIB may deploy
5468 with and form the core of the tactical unit's OSINT organization as well as provide the control mechanism
5469 for synchronization and information exchange between echelons.

5470 **OPEN-SOURCE INTELLIGENCE CONSIDERATIONS**

5471 11-7. For the most part, the considerations for OSINT are similar to those of other intelligence disciplines.

- 5472 ● OSINT organizations need clearly stated intelligence requirements to effectively focus
5473 collection and production.
- 5474 ● OSINT operations must comply with AR 381-10 and Executive Order 12333 on the collection,
5475 retention, and dissemination information on US persons.
- 5476 ● OSINT organizations can be overwhelmed by the volume of information to process and analyze.
- 5477 ● OSINT operations require qualified linguists for foreign language-dependent collection and
5478 processing tasks.

5479 11-8. Personnel responsible for planning or executing OSINT operations must also consider the concerns
5480 discussed below.

FOR OFFICIAL USE ONLY

5481 **COMPLIANCE**

5482 11-9. Under AR 381-10, procedure 2, Army intelligence activities may collect publicly available
5483 information on US persons only when it is necessary to fulfill an assigned function. There must also be a
5484 link between the collection of the US person information and the Army intelligence organization's
5485 assigned mission. Army intelligence components must exhaust the least intrusive collection means before
5486 requesting a more intrusive collection means. The following are additional considerations for Internet
5487 collection:

- 5488 • Army intelligence components must use Government computers to access the Internet for
5489 official Government business unless otherwise authorized.
- 5490 • Internet protocol addresses, uniform resource locators (URLs), and email addresses that are not
5491 self-evidently associated with a US person may be acquired, retained, and processed by Army
5492 intelligence components without making an effort to determine whether they are associated with
5493 a US person as long as the component does not engage in analysis focused upon specific
5494 addresses. Once such analysis is initiated, the Army intelligence component must make a
5495 reasonable and diligent inquiry to determine whether the data are associated with a US person.

5496 **LIMITATIONS**

5497 11-10. Intelligence personnel and organizations must comply with applicable DOD Directives and Army
5498 Regulations that govern contact with and collection of information from open sources. For example, DOD
5499 Directive 5100.20 prohibits SIGINT organizations from collecting and processing information from public
5500 broadcasts with exception of processing encrypted or "hidden meaning" passages. AR 380-13 prohibits the
5501 assignment of Army personnel, military or civilian, to attend public or private meetings, demonstrations, or
5502 other similar activities held off-post to acquire CI investigative information without specific approval by
5503 the Secretary or the Under Secretary of the Army.

5504 **OPERATIONS SECURITY**

5505 11-11. More than any other intelligence discipline, the OSINT discipline could unintentionally provide
5506 indicators of US military operations. Information generally available to the public as well as certain
5507 detectable activities such as open-source research and collection can reveal the existence of, and sometimes
5508 details about, classified or sensitive information or undertakings. Such indicators may assist those seeking
5509 to neutralize or exploit US military operations. Purchasing documents, searching an Internet site, or asking
5510 questions at public events are examples of detectable open-source research and collection techniques that
5511 could provide indicators of US plans and operations.

5512 11-12. Taking OPSEC into consideration, organizations must determine what level of contact with open
5513 sources and which collection techniques might provide indicators that an enemy could piece together in
5514 time to affect US military operations. In OSINT operations, countermeasures range from limiting the
5515 frequency or duration of contact with a source to prohibiting all contact with a source. If OPSEC so
5516 requires, such as to protect a Government computer from hacker retaliation, a direct reporting unit
5517 commander may approve nonattributable Internet access.

5518 **CLASSIFICATION**

5519 11-13. AR 380-5 states that intelligence producers "must be wary of applying so much security that they
5520 are unable to provide a useful product to their consumers." This is an appropriate warning for OSINT
5521 operations where concern for OPSEC can undermine the ability to disseminate inherently unclassified
5522 information. As shown in table 11-1, the classification of source metadata, collector metadata, collected
5523 information, and derivative intelligence differs based on the means of collection and the degree of damage
5524 to national security that disclosure of this information could reasonably be expected to cause. Since it is
5525 already in the public domain, publicly available information and the source metadata are unclassified.
5526 AR 380-5, chapter 4, directs that Army personnel will not apply classification or other security markings

FOR OFFICIAL USE ONLY

5527 “to an article or portion of an article that has appeared in a newspaper, magazine, or other public medium.”
 5528 For reasons of OPSEC, the classification of collector information is controlled unclassified or classified
 5529 information.

5530 **Table 11-1. Open-source intelligence classification considerations**

IF		THEN			
Information Source	Collection Means	Source Metadata	Collector Metadata	Collected Information	Intelligence Report
Confidential	Overt	Classified or Controlled Unclassified	Classified or Controlled Unclassified	Classified or Controlled Unclassified Information	Classified or Controlled Unclassified
	Clandestine	Classified	Classified		
Open	Overt	Unclassified	Controlled Unclassified	Unclassified	Classified, Controlled Unclassified, or Unclassified
	Nonattributable		Classified or Controlled Unclassified		

NOTE: This table is prescriptive not directive. Organizations with original classification authority or personnel with derivative classification responsibilities must provide subordinate organizations and personnel with a security classification guide or guidance for information and intelligence derived from open sources in accordance with the policy and procedures in AR 380-5.

5531 11-14. According to AR 380-5, chapter 2, a compilation of unclassified publicly available information
 5532 into an intelligence product (estimate, report, or summary) is normally not classified. In unusual
 5533 circumstances, the combination of individual unclassified items of information into an intelligence product
 5534 may require classification if the compilation provides an added factor that warrants classification.

5535 11-15. AR 380-5, chapter 6, provides a list of factors or classification considerations which includes but
 5536 is not limited to the following:

- 5537 ● Intelligence that reveals the identity of a conventional source or method that normally does not
 5538 require classification.
- 5539 ● Intelligence identifying a sensitive source or method is classified, as well as the evaluation of the
 5540 particular source or method.
- 5541 ● An intelligence requirement is classified when it reveals what is not known, what is necessary to
 5542 know, and why.

5543 *Note.* The intelligence staff creates sanitized, unclassified collection tasks from the intelligence
 5544 requirements since uncleared US and non-US persons make up a significant portion of open
 5545 source collectors.

- 5546 ● Information that would divulge intelligence interests, value, or extent of knowledge on a subject.
- 5547 ● Information related to political or economic instabilities in a foreign country threatening
 5548 American lives and installation there.

FOR OFFICIAL USE ONLY

5549 DECONFLICTION

5550 11-16. During planning, the G-2/S-2 staff and the G-3/S-3 staff must deconflict OSINT operations with
 5551 other activities. Specifically, contact or interaction with open sources may compromise the operations of
 5552 another intelligence discipline. Open-source collection may adversely affect the ability of non-intelligence
 5553 organizations such as CA, MP, medical, and PA to accomplish their missions. Conversely, CA, MP,
 5554 medical, PA, or other personnel who overtly contact an OSINT source may inadvertently compromise
 5555 OSINT operations as well as the safety of the open source or collector. Each of these situations could lead
 5556 to the loss of access to the open source and information of intelligence value.

5557 DECEPTION AND BIAS

5558 11-17. Deception and bias are of particular concern in OSINT operations. Unlike other disciplines,
 5559 OSINT operations do not normally collect information by direct observation of activities and conditions
 5560 within the AO. OSINT operations rely on secondary sources to collect and distribute information that the
 5561 sources may not have observed themselves. Secondary sources such as government press offices,
 5562 commercial news organizations, NGO spokespersons, and other information providers can intentionally or
 5563 unintentionally add, delete, modify, or otherwise filter the information they make available to the general
 5564 public. These sources may also convey one message in English for US or international consumption and a
 5565 different non-English message for local or regional consumption. It is important to know the background
 5566 of open sources and the purpose of the public information in order to distinguish objective, factual
 5567 information from information that lacks merit, contains bias, or is part of an effort to deceive the reader.

5568 11-18. In addition to determining the reliability and validity of the information obtained during OSINT
 5569 operations, intelligence analysts must consider the biases and cultural backgrounds of civilian interpreters
 5570 who may be used to translate or even search for relevant non-English information. These civilian
 5571 interpreters may be local hires when deployed overseas, and many civilian interpreters do not have security
 5572 clearances.

5573 INTELLECTUAL PROPERTY

5574 11-19. AR 27-60 prescribes policy and procedures for the acquisition, protection, transfer and use of
 5575 patents, copyrights, trademarks, and other intellectual property by DA. It is Army policy to recognize the
 5576 rights of copyright owners consistent with the Army's unique mission and worldwide commitments. As a
 5577 general rule, Army organizations will not reproduce or distribute copyrighted works without the permission
 5578 of the copyright owner unless such use is within an exception under US Copyright Law or required to meet
 5579 an immediate, mission-essential need for which non-infringing alternatives are either unavailable or
 5580 unsatisfactory.

5581 11-20. According to the US Copyright Office, "fair use" of a copyrighted work for purposes such as
 5582 criticism, comment, news reporting, teaching, scholarship, or research, is not an infringement of copyright.
 5583 Implicit with fair use is the documentation and citation of the source of the copyrighted information. The
 5584 following are four factors in determining fair use:

- 5585 ● Purpose and character of the use. In the context of fair use, intelligence operations are similar in
 5586 purpose and usage to non-profit news reporting and research organizations.
- 5587 ● Nature of the copyrighted work.
- 5588 ● Amount and substantiality of the portion used in relation to the copyrighted work as a whole.
 5589 There is no specific number of words, lines, or notes that may safely be taken without
 5590 permission. Usually, the amount or portion of copyrighted material is limited to quotations of
 5591 excerpts and short passages, and summary of a speech or article, with brief quotations.
- 5592 ● Effect of the use upon the potential market for or value of the copyrighted work. The effect on
 5593 the market or value of copyrighted material relates to reproduction and dissemination of
 5594 products provided by the owner beyond that authorized the owner's "Terms of Use" or
 5595 described in contracts and licenses with the US Government.

FOR OFFICIAL USE ONLY

5596 **OPEN SOURCES AND INFORMATION**

- 5597 11-21. Open sources and publicly available information may include but are not limited to—
- 5598 ● **Academia.** Courseware, dissertations, lectures, presentations, research papers, and studies in
 - 5599 both hardcopy and softcopy on economics, geography (physical, cultural, and political-military),
 - 5600 international relations, regional security, science, and technology.
 - 5601 ● **Governmental, Intergovernmental, and NGOs.** Databases, posted information, and printed
 - 5602 reports on a wide variety of economic, environmental, geographic, humanitarian, security,
 - 5603 science, and technology issues.
 - 5604 ● **Commercial and Public Information Services.** Broadcasted, posted, and printed news on
 - 5605 current international, regional, and local topics.
 - 5606 ● **Libraries and Research Centers.** Printed documents and digital databases on a range of topics
 - 5607 as well as knowledge and skills in information retrieval.
 - 5608 ● **Individuals and Groups.** Handwritten, painted, posted, printed, and broadcasted information
 - 5609 (for example, art, graffiti, leaflets, posters, and websites).

5610 **OPEN-SOURCE MEDIA**

5611 11-22. A simple communications model consists of a sender, a message, a medium, and a receiver. The

5612 medium is the access point to publicly available information for open-source research and collection. The

5613 primary media that open sources use to communicate information to the general public are shown in

5614 table 11-2 and discussed below.

5615 **PUBLIC SPEAKING FORUMS**

5616 11-23. Public speaking, the oldest medium, is the oral distribution of information to audiences during

5617 events that are open to the public or occur in public areas. These events or forums include but are not

5618 limited to academic debates, educational lectures, news conferences, political rallies, public government

5619 meetings, religious sermons, and S&T exhibitions. Neither the speaker nor the audience has the

5620 expectation of privacy when participating in a public speaking forum unless there is an expressed condition

5621 of privacy such as the Chatham House Rule. The Chatham House Rule says that:

5622 *When a meeting, or part thereof, is held under the Chatham House Rule, participants are*

5623 *free to use the information received, but neither the identity nor the affiliation of the*

5624 *speaker(s), nor that of any other participant, may be revealed.*

5625 11-24. If invoked, privacy conditions such as the Chatham House Rule change the characterization of the

5626 source from an open to a confidential source and may necessitate treating the source and collected

5627 information in accordance with HUMINT or CI procedures. Unlike the other open-source collection,

5628 monitoring public speaking events is done through direct observation and, due to its overt nature, could

5629 entail risk to the collector.

5630 **PUBLIC DOCUMENTS**

5631 11-25. A document is any recorded information regardless of its physical form or characteristics. Like

5632 public speaking, public documents have always been a source of intelligence. Documents provide in-depth

5633 information about the operational environment that underpin our ability to plan, prepare for, execute, and

5634 assess military operations. During operations, documents such as newspapers and magazines provide

5635 insights into the effectiveness of information tasks, especially information engagement. Books, leaflets,

5636 magazines, maps, manuals, marketing brochures, newspapers, photographs, public property records, and

5637 other forms of recorded information continue to yield information of intelligence value about operational

5638 environments. Sustained document collection contributes to the development of studies about potential

5639 operational environments. Collection of documents on the operational and technical characteristics of

5640 foreign materiel aid in the development of improved US tactics, countermeasures, and equipment.

FOR OFFICIAL USE ONLY

Table 11-2. Primary open-source media

SYSTEM	COMPONENTS	ELEMENTS
PUBLIC SPEAKING	SPEAKER	<ul style="list-style-type: none"> • Sponsor • Relationship • Message
	FORMAT	<ul style="list-style-type: none"> • Conference • Debate • Demonstration • Lecture • Rally
	AUDIENCE	<ul style="list-style-type: none"> • Location • Composition
PUBLIC DOCUMENTS	GRAPHIC	<ul style="list-style-type: none"> • Drawing • Engraving • Painting • Photograph • Print
	RECORDED	<ul style="list-style-type: none"> • Compact Data Storage Device • Digital Video Disk • Hard Disk • Tape
	PRINTED	<ul style="list-style-type: none"> • Book • Brochure • Newspaper • Periodical • Pamphlet • Report
PUBLIC BROADCASTS	RADIO	<ul style="list-style-type: none"> • Low Frequency AM Radio • Medium Frequency AM Radio • VHF FM Radio • L- and S-Band Satellite Radio
	TELEVISION	<ul style="list-style-type: none"> • Ku Band Satellite Television • VHF and UHF Terrestrial Television
INTERNET SITES	COMMUNICATIONS	<ul style="list-style-type: none"> • Chat • Email • News; Newsgroup • Webcam • Webcast • Weblog
	DATABASES	<ul style="list-style-type: none"> • Commerce • Education • Government • Military Organizations

FOR OFFICIAL USE ONLY

5641

Table 11-2. Primary open-source media (continued)

<i>SYSTEM</i>	<i>COMPONENTS</i>	<i>ELEMENTS</i>
INTERNET SITES (continued)	INFORMATION (WEBPAGE CONTENT)	<ul style="list-style-type: none"> • Commerce • Education • Government • Military Organizations
	SERVICES	<ul style="list-style-type: none"> • Dictionary • Directory • Downloads • Financial • Geospatial • Search and URL Lookup • Technical Support • Translation

5642 **PUBLIC BROADCASTS**

5643 11-26. A public broadcast entails the simultaneous transmission of data or information for general public
5644 consumption to all receivers or terminals within a computer, radio, or television network. Public broadcasts
5645 are important sources of current information about the operational environment. Television news
5646 broadcasts often provide the first I&W of situations that may require the use of US forces. Broadcast news
5647 and announcements enable personnel to monitor conditions and take appropriate action when conditions
5648 change within the AO. News, commentary, and analysis on radio and television also provide windows into
5649 how governments, civilians, news organizations, and other elements of society perceive the US and US
5650 military operations. Broadcasts also provide information and insights into the effectiveness of information
5651 tasks.

5652 **INTERNET SITES**

5653 11-27. Army intelligence components must use Government computers to access the Internet for official
5654 Government business unless otherwise authorized (for example, an Army Reservist participating in the
5655 World Basic Information Library Program).

5656 11-28. Internet sites enable users to participate in a publicly accessible communications network that
5657 connects computers, computer networks, and organizational computer facilities around the world. The
5658 Internet is more than just a research tool. It is an ISR tool that enables intelligence personnel to locate and
5659 observe open sources of information. Through the Internet, trained collectors can detect and monitor
5660 Internet sites that may provide I&W of enemy intentions, capabilities, and activities.

5661 11-29. Collectors can monitor newspaper, radio, and television websites that support assessments of
5662 information tasks, especially information engagement. Collectors can conduct periodic searches of
5663 webpages and databases for content on threat characteristics. Collecting webpage content and links can
5664 provide useful information about relationships between individuals and organizations. Properly focused,
5665 collecting and processing publicly available information from Internet sites can support understanding of
5666 the operational environment.
5667

FOR OFFICIAL USE ONLY

5668

Chapter 12

5669

Signals Intelligence

5670

DEFINITION

5671

12-1. *SIGINT is intelligence produced by exploiting foreign communications systems and noncommunications emitters (JP 2-0).* SIGINT provides unique intelligence information, complements intelligence derived from other sources, and is often used for cueing other sensors to potential targets of interest. For example, SIGINT which identifies activity of interest may be used to cue GEOINT to confirm that activity. Conversely, changes detected by GEOINT can cue SIGINT collection against new targets. The discipline is subdivided into three subcategories: communications intelligence (COMINT), electronic intelligence (ELINT), and foreign instrumentation signals intelligence (FISINT).

5672

5673

5674

5675

5676

5677

5678

- COMINT is intelligence and technical information derived from collecting and processing intercepted foreign communications passed by radio, wire, or other electromagnetic means. COMINT includes computer network exploitation, which is gathering data from target or adversary automated information systems or networks. COMINT also may include imagery, when pictures or diagrams are encoded by a computer network or radio frequency method for storage and/or transmission. The imagery can be static or streaming.

5679

5680

5681

5682

5683

5684

- ELINT is intelligence derived from the interception and analysis of noncommunications emitters (for example, radar). ELINT consists of two subcategories: operational ELINT (OPELINT) and technical ELINT (TECHELINT).

5685

5686

5687

- OPELINT is concerned with operationally relevant information such as the location, movement, employment, tactics, and activity of foreign noncommunications emitters and their associated weapon systems.

5688

5689

5690

- TECHELINT is concerned with the technical aspects of foreign noncommunications emitters such as signal characteristics, modes, functions, associations, capabilities, limitations, vulnerabilities, and technology levels.

5691

5692

5693

- FISINT involves the technical analysis of data intercepted from foreign equipment and control systems such as telemetry; electronic interrogators; tracking, fusing, arming, firing command systems, and video datalinks.

5694

5695

5696

ROLE

5697

12-2. SIGINT provides intelligence on threat capabilities, disposition, composition, and intentions. In addition, SIGINT provides targeting information for the delivery of lethal and nonlethal fires. Ultimately, the role of SIGINT is to collect, process, and disseminate SIGINT information in support of operations.

5698

5699

5700

FUNDAMENTALS

5701

12-3. It is important that the G-2/S-2 understand how SIGINT assets are organized not only within the Army but also throughout DOD. The majority of SIGINT assets from all the armed services, combined with national SIGINT assets, work together to support commanders from the tactical to the strategic level. Only by understanding the SIGINT structure that transcends traditional service component boundaries can the

5702

5703

5704

5705

5706

G-2/S-2 understand how to use SIGINT effectively.

FOR OFFICIAL USE ONLY

5707 **NATIONAL TACTICAL SIGINT RELATIONSHIPS**

5708 12-4. Since September 11, 2001, National Tactical SIGINT integration has grown from concept to reality.
5709 Today, tactical Army SIGINT elements rely heavily on NSA for many integrated functions and,
5710 conversely, NSA relies on tactical resources for intelligence. These functions and interfaces include NSA
5711 network (NSANet) connectivity to conduct analytic and data exchanges and input data into and access raw
5712 data from databases, and supporting the Army SIGINT collectors and analysts with specific SIGINT
5713 equipment and tools. Intelligence development has increased to the point of truly being integrated within
5714 the SIGINT enterprise. The SIGINT technical architecture complements existing C2 relationships; it does
5715 not replace the commander's authority or chain of command. The following organizations are the basis for
5716 this relationship.

5717 **ARMY CRYPTOLOGIC OPERATIONS, INSCOM**

5718 12-5. Army Cryptologic Operations (ACO) is an element of INSCOM G-2 located within NSA and acts as
5719 the Army's Service cryptologic element (SCE) representative. ACO supports Army cryptologic operations,
5720 capabilities, and resourcing for the purpose of providing dominant strategic and operational SIGINT,
5721 Information Assurance, and Information Operations for ground component commanders, national agencies,
5722 and national decision makers. The ACO is instrumental in providing SIGINT quick reaction capability
5723 systems. The ACO works closely with NSA and other SCEs to collaborate and leverage the SIGINT
5724 enterprise in improving sensor capabilities and technical and analytical support to Army SIGINT elements.

5725 **ARMY TCAE (ATCAE)**

5726 12-6. The ATCAE, established at the national level, plays a significant role in TCAE operations by
5727 providing technical support oversight and coordinating collaborative issues such as getting approvals for
5728 NSA connectivity and access to national databases for US Army tactical SIGINT personnel. The ATCAE
5729 is located within the NSA complex at Fort Meade, MD, and represents the Army Deputy Chief of Staff for
5730 Intelligence on SIGINT technical matters involving Army ground SIGINT elements.

5731 12-7. The ATCAE works closely with the Army Cryptologic Operations to support the Army's special
5732 sensor capabilities by providing SIGINT technical and analytical support. The special sensor capability
5733 systems are responsive to the ground force commander's requirements and enable SIGINT personnel to
5734 conduct SIGINT operations against modern communications systems.

5735 2-118. The ATCAE provides 24-hour service through its service desk and time-sensitive operations or
5736 military support desks. This support includes—

- 5737 ● Comprehensive technical SIGINT information to support collection, processing, analysis, and
5738 reporting, as well as collateral support for the unit's SIGINT/EW mission.
- 5739 ● Information on current world situations and friendly and threat military operations, tailored to a
5740 given unit's mission.
- 5741 ● Assistance in identifying hardware and software to carry out specific training and operational
5742 missions beyond the capability of organic equipment and systems.
- 5743 ● Advising Army tactical SIGINT personnel, at all levels, to reach and maintain an operational
5744 readiness posture by using ATCAE mobile training teams MTTs, the TROJAN program, and
5745 SIGINT Foundry Garrison Cryptologic Activities assets.
- 5746 ● Electronic quality control of unit reporting and forwarding to national time-sensitive systems.
- 5747 ● Assistance in obtaining SIGINT communications network connectivity and accesses to national
5748 assets to include databases.
- 5749 ● Assistance in reviewing and recommending modifications to US SIGINT directives on behalf of
5750 the tactical ground units' SIGINT technical issues.

5751

FOR OFFICIAL USE ONLY

5752 **SIGINT FOUNDRY**

5753 12-8. Soldiers deploying to operational zones will continue to face new technologies which they must
 5754 exploit, process, analyze, and report. AIT training will provide foundational training, but Soldiers require
 5755 more extensive training to ready them for specific deployments. The Army developed SIGINT Foundry to
 5756 meet new SIGINT requirements and to bring SIGINT Soldiers up to operational readiness prior to
 5757 deployment. As a result of close coordination between the Army G-2, the ACO/INSCOM, and the 704th
 5758 MI Bde/742d MI Bn (ATCAE), nine Garrison Cryptologic Activity Centers are being established at the
 5759 major CONUS Army installations to provide both training and overwatch capabilities to bring Army
 5760 SIGINT Soldiers to an operational readiness standard.

5761 **THEATER TCAE**

5762 12-9. The theater TCAE performs SIGINT technical control and analysis and management. It provides
 5763 SIGINT technical support for assigned, attached, OPCON, and lower echelon SIGINT resources deployed
 5764 in the AOR. This includes mission tasking, processing, analyzing, and reporting of SIGINT data,
 5765 information, and intelligence. The TCAE provides direction for the theater C&E battalion's SIGINT
 5766 mission and for other theater tactical SIGINT assets.

5767 **ARMY SIGINT SYSTEMS**

5768 12-10. SIGINT elements at echelons corps and below conduct actions to search for, intercept, and
 5769 identify threat signals for the purpose of immediate recognition. These actions provide information
 5770 required to answer PIRs and other intelligence requirements in support of the ISR effort.

5771 12-11. There is a varying mixture of SIGINT assets at echelons corps and below that include—

- 5772 ● AN/TSQ-219(V1 and V2), Tactical Exploitation System.
- 5773 ● AN/PRD-13(V2), Improved SIGINT Man-pack System.
- 5774 ● AN/MLQ-4X, Prophet and AN/MSW-24 Prophet Control.
- 5775 ● AN/USD-9, Guardrail Common Sensor.
- 5776 ● AN/ASQ-223, Airborne Reconnaissance Low-Multifunction.

5777 12-12. For more information on SIGINT assets, see MIHB 2-50.

5778 **SIGNALS INTELLIGENCE IN THE INTELLIGENCE PROCESS**

5779 12-13. The SIGINT discipline has several unique considerations throughout the steps of the intelligence
 5780 process.

5781 **GENERATE INTELLIGENCE KNOWLEDGE**

5782 12-14. SIGINT personnel conduct intelligence reach; research (for example, databases, academic studies,
 5783 products, or materials, OSINT or other information sources); and data mining that aid in determining the
 5784 adversary's use of the electromagnetic spectrum in the supported unit's AOI. SIGINT personnel must
 5785 follow all applicable policies and regulations on the collection of information and OPSEC. The information
 5786 and intelligence gathered is the basis for—

- 5787 ● Developing a comprehensive SIGINT baseline database for the AO. What communications
 5788 means does the threat use and what are their TTP? Do they incorporate civilian systems with
 5789 military systems?
- 5790 ● Determining key SIGINT collection gaps. Are all the threat's electromagnetic emanations being
 5791 collected and results databased? If not, why? If they are being collected, how do we receive or
 5792 pull the reporting?

FOR OFFICIAL USE ONLY

- 5793
- 5794
- 5795
- 5796
- 5797
- 5798
- Developing an understanding of the information and intelligence that can be collected with unit SIGINT collection assets and, when appropriate, other SIGINT collection assets in the AO. This also includes how and where the threat emanations may best be collected. Does the terrain support line of sight collection and reporting communications systems?
 - Determining a method of understanding when changes to the baseline occur that are of intelligence interest. Does the threat go to radio silence prior to an offensive operation?

5799

5800

5801

5802

5803

12-15. This information also can be used to determine predeployment training and develop exercises to provide as realistic and relevant training as possible. For tactical SIGINT personnel the best means to generate intelligence knowledge is by conducting tactical overwatch. While conducting tactical overwatch the SIGINT personnel, for example, will know what the specific types of threats, threat equipment, and threat TTP that they can expect to encounter when deployed.

5804 **PLAN**

5805

5806

5807

12-16. An important SIGINT planning consideration is that, when possible, SIGINT collection should be employed in conjunction with other intelligence disciplines collection systems. SIGINT is often used to cue, and be cued by, other ISR assets.

5808

5809

5810

12-17. During planning, the SIGINT technical control element retrieves, updates, and develops any required SIGINT databases. This includes coordination with air and ground assets, other SIGINT assets or elements that support the operation, as well SIGINT assets that will operate in other units AO.

5811 **PREPARE**

5812

5813

5814

5815

12-18. Preparation involves operational direction and control of SIGINT activities, including tasking and the allocation of effort. Operational control of SIGINT assets provides an authoritative prescription for SIGINT activities to include the uniform techniques and standards by which SIGINT information is collected, processed, and reported.

5816

5817

5818

12-19. SIGINT operational tasking encompasses the direct levying of SIGINT information requirements by a military commander on designated SIGINT resources. This includes the authority to deploy all or part of the SIGINT resources for which SIGINT operational tasking authority has been delegated.

5819

5820

5821

12-20. The commander ensures the SIGINT unit and asset leaders have conducted all necessary coordination and rehearsals. This includes establishing or verifying the operation of the SIGINT technical architecture.

5822

5823

5824

5825

5826

12-21. The G-2/S-2 and SIGINT asset commander validate the availability of SIGINT assets and resources. SIGINT reporting and dissemination channels and procedures need to be in place. Deploying personnel require deployment training and a current polygraph in order to qualify for access to resources; appropriate and necessary database access; and connectivity and interoperability with all appropriate SIGINT elements. Courses such as Deployer (DEPL) 2000 help prepare SIGINT Soldiers for deployment.

5827 **COLLECT**

- 5828
- 5829
- 5830
- 5831
- 5832
- 5833
- 5834
- 5835
- 5836
- 12-22. SIGINT performs two major collection activities:
- **Signals Intercepts:** These include those SIGINT actions used to search for, intercept, and identify threat electromagnetic signals for the purpose of immediate threat recognition. Signals intercept provides information required to answer PIRs and other intelligence requirements in support of the ISR effort.
 - **Direction Finding:**
 - Even when threat radio operators use COMSEC procedures, SIGINT teams can often intercept and approximate the location of the threat's signals. SIGINT teams can use DF to determine the movement of threat personnel or equipment; locations of emitters associated

FOR OFFICIAL USE ONLY

5837 with weapon systems and units; new and confirmed emitter locations; and possible friendly
5838 targets the enemy intends to attack (lethal and nonlethal).

5839 ■ In addition to using DF to intercept and approximate the location of threat forces, DF
5840 operations can assist the (radio-equipped) friendly force by locating and vectoring assets or
5841 units during limited visibility; locating downed aircraft and personnel radio beacons;
5842 conducting signal security assessments; and locating sources of communication
5843 interference and jamming.

5844 12-23. SIGINT processing involves converting intercepts of signals into written and verbal reports,
5845 automated message, graphic displays, recordings, and other forms suitable for analysis and intelligence
5846 production. Since US forces routinely conduct operations against threats who speak languages other than
5847 English, SIGINT processing often also includes translation of these intercepts.

5848 12-24. Due to the complexity of many SIGINT systems, automated processing may occur several times
5849 before SIGINT data or information receives any human interaction.

5850 ELECTRONIC WARFARE SUPPORT AND SIGINT

5851 12-25. EW refers to any military action involving the use of electromagnetic or directed energy to control
5852 the electromagnetic spectrum or to attack the adversary (JP 3-51). SIGINT is often confused or
5853 misrepresented as EW or a subdivision of EW known as electronic warfare support (ES). ES is achieved by
5854 **assets tasked or controlled by an operational commander**. These assets are tasked to search for,
5855 intercept, identify, and locate or localize sources of intentional or unintentional radiated electromagnetic
5856 energy. The purpose of ES tasking is immediate threat recognition, planning and conduct of future
5857 operations, and other tactical actions such as threat avoidance, targeting, and homing.

5858 12-26. ES is intended to respond to an immediate operational requirement. However, the same assets and
5859 resources that are tasked with ES can simultaneously collect intelligence that meets other collection
5860 requirements. That is not to say that data collected for intelligence cannot meet immediate operational
5861 requirements. Intelligence collected for ES purposes is normally also processed by the appropriate parts of
5862 the intelligence community for further exploitation after the operational commander's ES requirements are
5863 met (JP 3-13.1).

5864 12-27. SIGINT can support and be supported by the components of EW. This means preserving the
5865 electromagnetic spectrum for friendly use while denying its use to the adversary. ES data can be used to
5866 produce SIGINT; this provides intelligence information for electronic or lethal attack or targeting.

5867 PRODUCE

5868 12-28. The SIGINT analyst provides SIGINT products to satisfy the associated intelligence requirements,
5869 in the required format and in a timely manner. The quality and timeliness of SIGINT products are highly
5870 dependent upon the type of intercept, the collection system, the system's position in relation to the threat
5871 emitter, the weather, as well as the SIGINT operator's ability to identify the appropriate threat signal
5872 activity. The objective for SIGINT is to be used in an all-source analytical approach.

5873 12-29. There are a number of products generated from SIGINT. SIGINT reports are time-sensitive in
5874 nature and will contain anything from a traditional text formatted report to nontraditional reports comprised
5875 of color graphics, sound and/or video clips. SIGINT reports produced have titles such as (although not
5876 limited to) klieglights, tactical reports, and tactical ELINT reports and contain caveats that allow or restrict
5877 intelligence information to individuals with a need to know.

5878 ANALYZE

5879 12-30. The SIGINT analyst evaluates intelligence and information about the enemy's communications
5880 capabilities to determine appropriate SIGINT collection strategies. Conversely, a corresponding analysis of
5881 the friendly forces' SIGINT capabilities must be conducted to ensure the continued effectiveness of, or to

FOR OFFICIAL USE ONLY

5882 improve upon, SIGINT collection. SIGINT analysts also sort through large amounts of SIGINT and
5883 information and intelligence to identify and use only that which pertains to the CCIRs (PIRs and FFIRs).

5884 **ASSESS**

5885 12-31. The primary goal of the assess function when applied to SIGINT is to determine whether the
5886 results of SIGINT collection meet the requirements of the unit's ISR effort. SIGINT producers must assess
5887 all facets of SIGINT operations, from receipt of the ISR task to the dissemination of SIGINT to determine
5888 effectiveness. This assessment is not only directed at SIGINT assets on an individual basis but also
5889 throughout the supporting SIGINT architecture and the unit's entire ISR effort.

5890 12-32. The G-2/S-2 immediately assesses SIGINT products upon receipt for timeliness, relevance, and
5891 accuracy. They must inform the SIGINT producer of the extent to which the product answered the PIR or
5892 intelligence requirement. Feedback is provided to the SIGINT producer and collector; this reinforces the
5893 effectiveness and efficiency of SIGINT.

5894 **PROPAGATE**

5895 12-33. SIGINT of critical importance to the force, including answers to the CCIRs (PIRs and FFIRs), is
5896 propagated and disseminated via the most expeditious means possible. Due to the highly perishable nature
5897 of SIGINT, the most expeditious reporting means is often immediately augmented with a follow-up report
5898 or augmented by a report transmitted through additional means, enhancing the probability of receipt.
5899 Sometimes the most expeditious means of reporting critical SIGINT information to the commander is face
5900 to face.

5901 12-34. For intelligence reach operations, SIGINT products are available and disseminated in a variety of
5902 forms: hardcopy, softcopy, direct viewing, or broadcast. Time-sensitive reporting keeps NSA,
5903 commanders, and, non-SIGINT organizations advised on the status of current and potential threats. It is
5904 imperative to ensure that SIGINT products are only transmitted over communications systems at the
5905 appropriate classification level.

FOR OFFICIAL USE ONLY

5906

Chapter 13

5907

Technical Intelligence

5908

DEFINITION

5909

13-1. TECHINT is derived from the collection, processing, analysis, and exploitation of data and information pertaining to foreign equipment and materiel for the purposes of preventing technological surprise, assessing foreign scientific and technical capabilities, and developing countermeasures designed to neutralize any adversary's technological advantages (JP 2-0).

5910

5911

5912

5913

ROLE

5914

13-2. A strength of the US military is the diversity and extent of its technology base. While the US is one of the world leaders in integrating technology, the threat can achieve temporary technological advantage in certain areas by acquiring modern systems or by improvising new weapons. The world arms market is willing to provide advanced systems to countries or individuals with the resources to pay for them. A concerted TECHINT enterprise is vital to providing precise direction and purpose to DOD R&D and exploitation process to ensure quick and efficient neutralization of threat technological advantages and networks.

5915

5916

5917

5918

5919

5920

5921

13-3. The role of TECHINT is to ensure that the warfighter understands the full technological capabilities of the threat. With this understanding, the US forces can adopt appropriate countermeasures, operations, and tactics.

5922

5923

5924

13-4. TECHINT has three goals within its role:

5925

- To ensure the US armed forces maintain technological advantage against any threat.
- To provide timely, relevant, accurate, predictive, and tailored TECHINT support to the warfighter throughout the full spectrum of military operations. This includes providing US forces intelligence, information, and training on foreign weapons systems to an extent that allows their use of CEE.
- To provide analysis of certain design traits of foreign weapons systems as indicators of threat intent.

5926

5927

5928

5929

5930

5931

5932

13-5. TECHINT includes the subset Weapons Technical Intelligence (WTI), which combines forensic science with TECHINT for application against irregular and nontraditional threats. As such, WTI has four goals:

5933

5934

5935

- To forensically examine events and/or devices or weapons to better understand linkages between technical design and tactical use to guide efforts of the protection warfighting function.

5936

5937

- To enable targeting by identifying, selecting, prioritizing, and tracking individuals and matching them with groups, weapons materiel, financiers, suppliers, insurgent leaders, and other related elements.

5938

5939

5940

- To provide forensic analysis of IEDs, improvised weapons, and weapon components to identify the origin of materiel and components.

5941

5942

- To utilize materiel collected during site exploitation activities to further detain and potentially prosecute individuals for criminal activity.

5943

FOR OFFICIAL USE ONLY

5944 **FUNDAMENTALS**

5945 13-6. The fundamentals of TECHINT consist of TECHINT/WTI application in the full spectrum of
5946 operations and the importance of chain of custody. See FM 2-22.4 for more information.

5947 **TECHINT/WTI APPLICATION IN FULL SPECTRUM OPERATIONS**

5948 13-7. TECHINT assets are capable of responding to threats throughout the full spectrum of operations.
5949 Traditional TECHINT capabilities are best suited to meet the needs of commanders in General war. For
5950 example, the equipment used in General war consists of traditional threat weapons systems (for example,
5951 tanks, missiles, ATGMs). As such, TECHINT is capable of quickly identifying the visible and other
5952 indications of new weapons, improved munitions or modifications that could potentially defeat US
5953 equipment.

5954 13-8. The knowledge gained, through TECHINT exploitation and analysis, also provides the necessary
5955 intelligence reach capability for operations that include lower levels of violence. Unlike general warfare,
5956 threat forces are not easily identified and often nontraditional and/or irregular threats take refuge in plain
5957 sight. Though the combination of forensic science and TECHINT, WIT provides commanders the ability to
5958 identify threat networks and their members. This is accomplished by linking individuals with events and
5959 materials that are intended to do harm to US forces. Indisputably, WTI assumes primacy in operations
5960 related to stable peace through insurgency.

5961 13-9. TECHINT and WTI can be used simultaneously when commanders anticipate or encounter a mix set
5962 of threats. Also, the unique capabilities of WTI can be scaled to complete missions related to high priority
5963 objectives in general war; for example, the detainment of government officials, political party leaders,
5964 military commanders, scientists, and engineers. These detainments can significantly shape the operations
5965 by informing commanders on threat equipment capabilities and can affect planning in persistent conflicts,
5966 when level of violence decreases.

5967 **CHAIN OF CUSTODY**

5968 13-10. The proper documentation of captured enemy equipment (CEE) and captured enemy materiel
5969 (CEM) is a key factor in producing accurate and relevant TECHINT for the commander. For example, the
5970 capture location or the employment of material and associated material can link significant point of interest
5971 that can yield exploitable information.

5972 13-11. Specifically, the proliferation of weapons from nation states and non-state actors can reveal third-
5973 party influences; properly recorded weapons emplacement can identify the effectiveness of weapons
5974 against US forces; and DOCEX can identify new tactics of weapon employment thus increasing
5975 effectiveness. Additionally, proper chain of custody is necessary in linking individuals and threat networks
5976 with weapons and material and/or events. The information gained through exploitation may eventually be
5977 used in US or HN legal proceedings.

5978 **THE TECHINT ENTERPRISE**

5979 13-12. The TECHINT enterprise consists of multiple entities within the Army working in concert with
5980 organizations from other Services components, within DOD, other US departments, national laboratories,
5981 and US academic institutions as well as international partners. For additional information on the TECHINT
5982 enterprise, see FM 2-22.4.

5983 **DEFENSE INTELLIGENCE AGENCY**

5984 13-13. DIA manages and reviews overall TECHINT activities. The S&TI Directorate within DIA is the
5985 action element for TECHINT. This directorate coordinates with external TECHINT agencies on non-policy
5986 matters concerning the production of S&TI. The following organizations provide TECHINT support under
5987 the control of DIA:

FOR OFFICIAL USE ONLY

- 5988 • **National Center for Medical Intelligence (NCMI)** based at Fort Detrick, MD, is a DOD
5989 intelligence production center under DIA control. NCMI is responsible for exploiting foreign
5990 medical materiel. The director supports the Army Foreign Materiel Program (FMP) and Army
5991 medical R&D requirements. The director coordinates planning, programming, and budgeting
5992 with the Army DCS, G-2.
- 5993 • **Missile and Space Intelligence Center (MSIC)** based at Redstone Arsenal, AL, is a DOD
5994 intelligence production center under DIA control and supports the FMP. The MSIC acquires,
5995 produces, maintains, and disseminates S&TI pertaining to missile and space weapons systems,
5996 subsystems, components, and activities. The S&TI produced at MSIC also covers foreign state-
5997 of-the-art technology and research applicable to missiles.
- 5998 • **Defense HUMINT** conducts worldwide HUMINT operations in support of foreign materiel
5999 acquisition (FMA) and foreign materiel exploitation (FME).

6000 13-14. The organizations and agencies below constitute the Army TECHINT structure.

6001 **HEADQUARTERS, DEPARTMENT OF THE ARMY DCS, G-2**

6002 13-15. HQDA DCS, G-2 exercises staff responsibility for all Army TECHINT activities. The Army DCS,
6003 G-2 forms policies and procedures for S&TI activities, supervises and carries out the Army S&TI program,
6004 coordinates DA staff and MSC requirements for TECHINT, and is responsible for the Army FMP.

6005 **US ARMY INTELLIGENCE AND SECURITY COMMAND**

6006 13-16. Under the direction of HQDA, INSCOM is responsible for TECHINT. INSCOM fulfills its
6007 responsibilities through its TECHINT oversight function and manages the Army's Foreign Materiel for
6008 Training (FMT) Program and FMP. It provides the interface with strategic S&TI agencies in support of
6009 FME and organizes, trains, and equips TECHINT organizations. TECHINT exploitation within INSCOM
6010 is performed by the following elements:

- 6011 • **National Ground Intelligence Center.** HQ, INSCOM, exercises OPCON over the NGIC.
6012 NGIC produces and maintains intelligence on foreign scientific developments, ground force
6013 weapons systems, and associated technologies. NGIC analysis includes but is not limited to
6014 military communications electronics systems, types of aircraft used by foreign ground forces,
6015 CBRNE capabilities, and basic research in civilian technologies with possible military
6016 applications. Recent additions to the NGIC mission include biometric intelligence data,
6017 databasing, and Counter Improvised Explosive Device Training Program (CITP).
- 6018 • **203d Military Intelligence Battalion.** The 203d MI Battalion is a multi-component unit
6019 headquartered at Aberdeen Proving Ground, MD, and is the Army's only TECHINT battalion. It
6020 performs the following functions:
 - 6021 ■ Forms the core of the Coalition Joint Captured Material Exploitation Center (CJCMEC).
6022 Provides logistics and infrastructure to absorb Joint and interagency TECHINT assets to
6023 form the CJCMEC.
 - 6024 ■ Conducts multiple CJCMEC missions worldwide.
 - 6025 ■ Conducts TECHINT collection and reporting in support of validated S&TI objectives.
 - 6026 ■ Conducts TECHINT training for DOD analysts and TECHINT personnel.
 - 6027 ■ Supports INSCOM's FMA and FME operations as directed.
 - 6028 ■ Analyzes and exploits foreign CEE, weapon systems, and other CEM.
 - 6029 ■ Reports on the capabilities and limitations of CEM.
 - 6030 ■ Provides recommendations for countermeasures to enemy technical advantages.
 - 6031 ■ Provides foreign or enemy equipment familiarization and training.
 - 6032 ■ Provides recommendations on the reuse of CEE.
 - 6033 ■ Responds to emerging TECHINT missions.

FOR OFFICIAL USE ONLY

- 6034 ■ Provides task-organized battlefield TECHINT teams to support the commander's
6035 TECHINT requirements.

6036 **US ARMY MATERIEL COMMAND**

6037 13-17. The US Army Materiel Command (AMC) plays a significant support role in TECHINT. Among
6038 AMC elements are a series of Army research, development, and engineering centers (RDECs), the Army
6039 Research Laboratory System, and the US Army Test and Evaluation Command. Each element plays a role
6040 in operations by conducting highly technical evaluations of foreign equipment.

6041 13-18. In time of persistent conflict, the AMC conducts FME on equipment purchased by each laboratory
6042 and by RDEC for the intelligence community and for DOD. AMC's foreign ordnance exploitation team,
6043 located at the Fire Support Armaments Center EOD (Picatinny Arsenal)—

- 6044 ● Exploits foreign ground ordnance.
6045 ● Develops render-safe procedures (RSP) for foreign ordnance.
6046 ● Prepares detailed intelligence reports to support EOD, intelligence, and US munitions developer
6047 communities.

6048 13-19. There are many other agencies with TECHINT responsibilities within the DOD. Refer to
6049 FM 2-22.4 for more information on TECHINT.

6050 **TECHNICAL INTELLIGENCE IN THE INTELLIGENCE PROCESS**

6051 13-20. The TECHINT discipline has several unique considerations throughout the steps of the
6052 intelligence process.

6053 **GENERATE INTELLIGENCE KNOWLEDGE**

6054 13-21. In order to preclude technological surprise on the battlefield, and to plan for countermeasures, US
6055 forces must conduct extensive research of joint knowledge databases with relevant intelligence on the
6056 threat. This does not only concern weapons the threat may possess but also other equipment, such as
6057 frequency hopping and spread spectrum communications, or sonar-elusive mini-submarines. Regardless of
6058 the technology, our forces must understand TECHINT characteristics and how the threat will employ
6059 technology in the AO long before they deploy into it. Only then can forces continue planning operations in
6060 accordance with the MDMP on an informed basis.

6061 13-22. For example, millions of tons of cached munitions from decades of war in locations like North
6062 Korea, Iran, Somalia, Afghanistan, and Iraq present a ready store of explosives for use in conventional or
6063 irregular warfare. Detailed TECHINT on the types of munitions, associated weapons systems, potential
6064 threat employment of munitions, as well as possible friendly use, and munitions locations is a key product
6065 of the generate intelligence knowledge task through intelligence reach of national and theater-level
6066 database access and data mining will form a key basis for developing a unit's initial intelligence survey. In
6067 turn, the intelligence survey will determine key TECHINT gaps, assist in understanding, allocating, and
6068 optimizing ISR assets for collection, and how to recognize and understand TECHINT developments which
6069 may affect US Soldiers in the AOs.

6070 13-23. Analysis prior to or after deployment into such an area mentioned above may determine that threat
6071 forces have access to numerous high explosive and chemical artillery rounds and are capable of detonating
6072 IEDs through various electronic means with deadly accuracy most likely resulting in high casualty rates.
6073 Counter-IED training in theater and at home station results in Soldier readiness and also prepares units with
6074 intelligence and knowledge to understand and attack insurgent networks. Unit and institutional training for
6075 TECHINT analysis teams provide a key combat multiplier as well as important links to knowledge centers
6076 through intelligence reach and DCGS-A. TECHINT databases serve units in contact as well as follow-on
6077 and redeployed units in support of ARFORGEN, particularly in terms of overwatch and lessons learned.

FOR OFFICIAL USE ONLY

6078 **PLAN**

6079 13-24. Based on the information or intelligence from the generate knowledge task, the G-2/S-2 refines
 6080 PIRs and information requirements including TECHINT considerations. Planning must include specialized
 6081 TECHINT support for both preplanned and contingency operations to ensure these teams are positioned in
 6082 accordance with operational needs. For example, a BCT commander’s PIRs and information requirements
 6083 may be, “How and where are munitions from other nations entering into the area of operations?” The BCT
 6084 S-2 coordinates ISR planning with the S-3 for sensitive border surveillance and reconnaissance from air,
 6085 ground, and water. TECHINT planning considerations include—

- 6086 ● Task-organizing ground reconnaissance units with TECHINT analysis teams or weapons
- 6087 intelligence teams (if available) with biometrics and forensics capabilities.
- 6088 ● Linguists for translation and transliteration.
- 6089 ● Intelligence reach capability to access and query databases and knowledge center analysts.
- 6090 ● IPB analysis indicating NAI and TAI based on an MCOO template.
- 6091 ● Joint capabilities ISR including SOF.

6092 13-25. As other mission requirements changes, TECHINT planning is synchronized with operations
 6093 according to commander’s guidance.

6094 **PREPARE**

6095 13-26. Training Soldiers is the basis for successful operations. The G-2/S-2 must ensure that required
 6096 TECHINT analytical assets, resources, and evacuation means are prepared to provide support. This
 6097 includes verifying coordination effected with the task-organized TECHINT teams from the 203d MI
 6098 Battalion. The G-2/S-2 must also ensure the means to report and disseminate TECHINT results to the unit
 6099 and its Soldiers are in place so they can immediately adopt appropriate countermeasures, operations, or
 6100 tactics in order to enhance their survival and mission accomplishment.

6101 13-27. Once an OPORD, OPLAN, or WARNO related to a TECHINT mission is issued, units may adjust
 6102 their planning and make further coordination with collaborative analytical and exploitation agencies to
 6103 augment their forces. In addition, the G-2/S-2 must ensure that required TECHINT analytical assets,
 6104 resources, and evacuation means are prepared to provide support.

6105 13-28. The G-2/S-2 must also ensure the means, such as DCGS-A, to report and disseminate TECHINT
 6106 results to the unit and its Soldiers are in place so they can immediately adopt appropriate countermeasures,
 6107 operations, or tactics in order to enhance their survival and mission accomplishment.

6108 **COLLECT**

6109 13-29. TECHINT collection includes capturing, reporting, and evacuating CEM. TECHINT collection
 6110 begins when an organization or individual reports the recovery or acquisition of threat materiel or as
 6111 ordered by a commander. An item of materiel is exploited at each level, and continues through succeeding
 6112 higher levels until an appropriate countermeasure to neutralize the item’s capabilities is identified or
 6113 developed.

6114 13-30. US forces safeguard CEM and report it through intelligence channels to the first TECHINT
 6115 element in the reporting chain. The location of this TECHINT element will be in accordance with the
 6116 METT-TC factors; however, the TECHINT representative or element will verify if the type of materiel is
 6117 of intelligence value and determine its further disposition in conjunction with the unit’s staff.

6118 **PROCESS**

6119 13-31. TECHINT processing starts (simultaneously with collection) with the capture of a piece of
 6120 equipment of TECHINT value. This confirms that the enemy is employing certain materiel of concern to

FOR OFFICIAL USE ONLY

6121 US forces. In accordance with METT-TC factors, a TECHINT team may move to the location of the item
6122 at the capture site or wait until the item is evacuated before conducting initial exploitation.

6123 13-32. After initial exploitation, the team decides if further processing is required. If it is, the items are
6124 sent to the JCMEC. If the item is deemed to yield no immediate tactical intelligence value, it may still be
6125 evacuated to the S&TI centers in CONUS for further analysis if the systems represent a change in the
6126 technological posture of an enemy.

6127 **PRODUCE**

6128 13-33. TECHINT teams normally report initial and secondary examinations of CEM using either a
6129 preliminary technical report or a complementary technical report.

- 6130 ● A preliminary technical report—
 - 6131 ■ Includes a general description of the item.
 - 6132 ■ Alerts others to information that can be used immediately by tactical units.
- 6133 ● A complementary technical report is more in-depth and—
 - 6134 ■ Follows a secondary or an in-depth initial examination.
 - 6135 ■ Allows the JCMEC to compare new information with intelligence holdings.

6136 13-34. At each successive echelon of exploitation, TECHINT analysts add to the overall body of
6137 information on an item by either adding to previous reports or by preparing new reports. The JCMEC or
6138 other national level S&TI activities prepare more advanced technical reports and analyses. These reports
6139 include—

- 6140 ● Detailed technical reports.
- 6141 ● Translation reports.
- 6142 ● Special technical reports.

6143 13-35. Other TECHINT products include—

- 6144 ● JCMEC publications such as operator manuals, maintenance manuals, TECHINT bulletins, and
6145 tactical user bulletins.
- 6146 ● S&TI analysis bulletins.
- 6147 ● FME reports.
- 6148 ● Weapons intelligence team reports.

6149 **ANALYZE**

6150 13-36. TECHINT analysts use checklists established by S&TI agencies and the JCMECs to analyze each
6151 type of the threat's equipment for which requirements exist. Analysis always begins with what is known,
6152 and what is not known, about the piece of equipment. TECHINT units maintain procedures and plans for
6153 sampling, analyzing, and handling materiel.

6154 **ASSESS**

6155 13-37. The primary goal of the TECHINT assess function is to determine whether the results of
6156 TECHINT production meet the unit's PIR or intelligence requirements. The G-2/S-2 immediately assesses
6157 TECHINT products upon receipt for timeliness, relevance, and accuracy. The G-2/S-2 must inform the
6158 TECHINT producer of the extent to which the product answered the PIR or intelligence requirement.
6159 Providing feedback to TECHINT analysts helps improve the effectiveness and efficiency of TECHINT.

6160 13-38. The G-2/S-2 also assesses the success of the unit's ISR effort in accomplishing any TECHINT-
6161 associated ISR task and shares the assessment with the staff and the pertinent units or personnel.

FOR OFFICIAL USE ONLY

6162 **PROPAGATE**

6163 13-39. TECHINT organizations post intelligence studies and TECHINT reports via secure Internet
 6164 databases as well as through existing intelligence communication architecture. When possible, the
 6165 preparing organizations share findings with other fusion and analysis elements for maximum effect.
 6166 Additionally, TECHINT contributes information about threat weapons and equipment and their
 6167 effectiveness against US forces, providing key input for the COP.

6168 13-40. Relevant TECHINT findings are shared with higher headquarters for operational and strategic
 6169 application; with adjacent units for pattern and trend analysis; and to lower echelons for situational
 6170 awareness and general knowledge. They are often used in the development of TTP. Direct dissemination of
 6171 information contained in TECHINT databases should be sent to the unit responsible for the capture and/or
 6172 collection of the material, connecting the technical expert with the operational and tactical commanders as
 6173 often as possible.

6174 13-41. TECHINT of critical importance to the force, including answers to the PIR, is disseminated via the
 6175 most expeditious means possible. Routine TECHINT reports and products are usually transmitted through
 6176 the unit's existing intelligence communications architecture in the format of a preliminary technical report.

6177 13-42. For intelligence reach operations, TECHINT products are available and disseminated in a variety
 6178 of forms. The requestor must ensure that the TECHINT product can be transmitted over the available
 6179 communications systems. This includes verifying the appropriate security level of the communications
 6180 systems.

FINAL DRAFT

FOR OFFICIAL USE ONLY

6181

Appendix A

6182

Example Intelligence Summary, Intelligence Estimate, and Intelligence Running Estimate Formats

6183

6184

INTELLIGENCE SUMMARY

6185

A-1. The intelligence summary (INTSUM) contains a brief summary of the most current enemy situation covering a period of time designated by the commander. This period of time will vary with the desires of the commander and the requirements of the situation. It provides a summary of the enemy situation, enemy operations and capabilities, and the characteristics of the terrain and weather and civil considerations.

6186

6187

6188

6189

A-2. The intelligence summary aids in assessing the current situation and updates other intelligence reports. Negative information is included, but no operational information is excluded. The INTSUM reflects the intelligence officer's interpretation and conclusions regarding threat capabilities and probable COAs. The INTSUM is prepared at brigade and higher echelons and disseminated to higher, lower, and adjacent units. The INTSUM has no prescribed format except the word "INTSUM" will be the first item of the report. Figure A-1 shows an example format of an INTSUM. This is neither an all-inclusive nor directed format.

6190

6191

6192

6193

6194

6195

6196

INTELLIGENCE ESTIMATE

6197

A-3. The primary purpose of the intelligence estimate is to—

6198

- Determine the COAs open to the threat and the probable order of their adoption.

6199

- Disseminate information and intelligence.

6200

- Determine PIRs concerning the threat and the AO.

6201

A-4. The intelligence estimate is a logical and orderly examination of the intelligence factors affecting the accomplishment of a mission. It provides commanders with an analysis of the AO and the threat strength and capabilities that can influence their mission. It is used as a basis for planning and disseminating intelligence.

6202

6203

6204

6205

A-5. An intelligence estimate may be prepared at any level. It may be written or oral, formal or informal, detailed or summarized. It is normally written at division and higher and briefed down to battalion. Figure A-2 shows an example format of an intelligence estimate. This is neither an all-inclusive nor directed format.

6206

6207

6208

FOR OFFICIAL USE ONLY

INTSUM FORMAT	
LINE 1 – DATE AND TIME _____	(DTG)
LINE 2 – UNIT _____	(Unit Making Report)
LINE 3 – SITUATION _____	(General Enemy Situation Since Last Report)
LINE 4 – ENEMY FLOT _____	(Current Enemy Front Line Trace)
LINE 5 – ENEMY UNIT SIZE _____	(Enemy Ground Maneuver Units LOCATION/ACTIVITY/Status by Echelon/Size, Location)Strength (Grid), Activity)
LINE 6 – ENEMY ARTILLERY _____	(Enemy Artillery Activity and Estimated Strength)
LINE 7 – ENEMY CBRNE _____	(Enemy CBRNE Activity (Type, Location, DTG))
LINE 8 – ENEMY AIR _____	(Enemy Air and Air Activity)
LINE 9 – ENEMY ENGINEER _____	(Enemy Engineer Activity)
LINE 10 – FORCE PROTECTION AREA THREAT _____	(Enemy FP Area Threat (Light Forces, SF))
LINE 11 – ENEMY'S EST COA _____	(Enemy's Most Probable Courses of Action)
LINE 12 – PIR _____	(Current PIR in Order of Priority and the Phase of Operation)
LINE 13 – ENEMY SUSTAINMENT _____	(Location and Activity of Enemy Combat Sustainment Units)
LINE 14 – VULNERABILITIES _____	(Combat Service Support Units)
LINE 15 – WEATHER AND TERRAIN _____	(Analysis of Enemy's Current or Emerging Vulnerabilities)
LINE 16 – ENEMY COMBAT ASSESSMENT _____	(Analysis of Effects of Weather and Terrain)
LINE 17 – NARRATIVE _____	(Summarize Enemy Combat Assessment During Period)
LINE 18 – AUTHENTICATION _____	(Free Text for Additional Information Required for Clarification of Report)
	(Report Authentication)

6209

Figure A-1. Example INTSUM format

FOR OFFICIAL USE ONLY

6210
6211
6212
6213
6214
6215
6216
6217
6218
6219
6220
6221
6222
6223
6224
6225
6226
6227
6228
6229
6230
6231
6232
6233

6234
6235
6236
6237
6238
6239
6240
6241
6242
6243
6244
6245
6246
6247
6248
6249
6250

Sample of a Division Intelligence Estimate

(Classification)
Copy No ____ of ____ Copies
G2 Section, 52d Infantry Division (Mech)
Glennville (NF3277), EASTLAND
230830Z June 19__

INTELLIGENCE ESTIMATE NO. 20

Reference: Map series EASTLAND, sheets DELTA through KILO, edition 2, 1:50,000.

1. **MISSION.** 52d Division conducts mobile defense along DRY CREEK, accepts no penetration south of HILLS 333 and 421, and prepares to conduct offensive operations within 12 hours.

2. **BATTLEFIELD AREA.**

a. Weather.

(1) Existing situation. Weather for the period 23 June to 28 June will be rainy, and cool, gradually warming and clearing as a high pressure system moves through the area of operations from the south. Temperatures from 40 degrees F to 65 degree F. Visibility will range from 16 to 25 kilometers, except during precipitation and in morning fog in low drainage areas. Surface winds from the south 8 to 10 knots.

<u>Date</u>	<u>BM- NT</u>	<u>BM- CT</u>	<u>EE- CT</u>	<u>EE- NT</u>	<u>Moon- Rise</u>	<u>Moon- Set</u>
23 Jun	0331	0419	2029	2130	1746	0125
25 Jun	0339	0422	2025	2124	1907	0214
27 Jun	0344	0425	2022	2118	2001	0518
28 Jun	0349	0428	2018	2112	2022	0820

(2) Effects on enemy courses of action:

(a) Precipitation will not hinder cross-country movement except in the low drainage areas of MINERTOWN.

(b) Southerly winds will not affect enemy employment of Nuclear Biological and Chemical.

(c) Low visibility during precipitation and morning fog will favor attack.

(3) Effects on friendly courses of action.

(a) Precipitation will not hinder cross-country movement except in the low drainage areas of MINERTOWN.

(b) Southerly wind direction will not affect friendly use of chemical or nuclear weapons.

(c) Low visibility during precipitation and morning fog will not favor friendly defense.

b. Terrain.

(1) Existing situation.

(a) Concealment and cover. Wooded areas around MIDWAY offer good concealment. Numerous ravines in drainage areas of MINERTOWN offer limited concealment and cover.

Figure A-2. Example format of an intelligence estimate

FOR OFFICIAL USE ONLY

6252 (b) Observation and fire. There are good observation points along bluffs above GRINGO River. Fields of
6253 fire are excellent throughout plains area north of MUD CREEK but limited moderately in populated and vegetated
6254 areas near GLENVILLE.
6255 (c) Obstacles.
6256 1 SWIFT River (fordable 1 kilometer east of GLENVILLE).
6257 2 Bluffs above GRINGO River.
6258 3 City of GLENVILLE. Routes around city are passable; routes through city are impassable.
6259 (d) Key terrain. Hill mass MUKELROY and HILL 333.
6260 (e) Avenues of approach.
6261 1 Available to the enemy into our sector:
6262 a Avenue of approach 1 is from LARGO through gap around the northeast end of HILL 702, 34
6263 kilometers southwest to MINERTOWN and south to DRY CREEK.
6264 b Avenue of approach 2 is from LARGO southeast through MIDWAY to river-crossing east of
6265 GLENVILLE.
6266 2 Avenue of approach available for US movement into enemy area will be generally the same as those
6267 listed for enemy into our sector.
6268 (2) Effect on enemy courses of action. Terrain favors the enemy attack using avenue of approach 1.
6269 (3) Effect on friendly courses of action. Terrain favors our defense of the area around DRY CREEK.
6270 c. Other Characteristics.
6271 (1) Existing situation. Local nationals throughout the area favor friendly military operations. Large
6272 numbers of refugees can be expected to pass through friendly lines.
6273 (2) Effect on enemy courses of action. The enemy can be expected to insert infiltrators as refugees.
6274 (3) Effect on friendly courses of action. Refugees can be expected to provide valuable intelligence.
6275 **3. ENEMY SITUATION.**
6276 a. Disposition. Annex A, Situation Overlay.
6277 b. Composition. Enemy forces opposing 52d Infantry Division(Mech) consist of elements of the 4th
6278 Combined Arms Army.
6279 (1) Identified units are:
6280 (a) 10 MRD consisting of:
6281 27th MRR
6282 30th MRR
6283 31st MRR
6284 121st TK Regt (unlocated)
6285 (b) 19th Mech Div Consisting of:
6286 23d MRR
6287 37th TK Regt
6288 (2) Unidentified units are: 2XU/IMRR of 19th MRD
6289 c. Strength.
6290 (1) Committed forces. 52d Infantry Division (Mech) is opposed immediately by 4 motorized rifle
6291 battalions and 1 tank battalion. These units are supported by normal divisional and regimental
6292 artillery.
6293 (2) Reinforcements. Reinforcements available to the enemy for commitment in our zone are a
6294 total of 5 motorized rifle battalions and 4 tank battalions from the 27th MRR, 121st TK Regt,
6295 and the second echelon battalions of the 30 and 31st MRRs and the 37 TK Regt. Also, the 23
6296 MRR can totally reinforce within 8 hours from start of movement.
6297 (3) Air. Enemy is supported by the 3d Air Army consisting of unidentified numbers of fighter-
6298 bomber aircraft, ground attack aircraft, and reconnaissance aircraft. Air parity currently exists
6299 with either force capable of obtaining air superiority for limited periods of time. Up to now
6300 enemy has used a maximum of 60 fighter-bomber sorties in a 12-hour period.
6301
6302
6303
6304
6305
6306
6307
6308

6309

Figure A-2. Example format of an intelligence estimate (continued)

FOR OFFICIAL USE ONLY

6310

6311 (4) Nuclear. No estimate of the enemy's nuclear support for the next 30 days is available.
6312 Enemy currently has 152mm Sp How with nuclear rounds and SSM which can deliver rounds
6313 of 10-50 KT yield within range of our division.

6314 d. Recent and Present Significant Activities.

6315 (1) Air reconnaissance and photo reports indicate increased enemy movement along axis
6316 BRAVO to LIMA. movement indicates reinforcement of forward element of 4th CAA.

6317 (2) Enemy's aerial recon and tactical air flights have increased in the last 36 hours, particularly
6318 in the line of contact.

6319 (3) For the past 36 hours, volume of vehicular traffic has increased in southerly direction.

6320 (4) Artillery fire from the enemy has become more intensive in the last 24 hours.

6321 (5) Reliable source reports large tracked, amphibious vehicles moving into area vicinity HILL
6322 805.

6323 (6) Enemy has begun to employ smoke along the forward slope of HILL 702.

6324 e. Peculiarities and Weaknesses.

6325 (1) Personnel. Enemy, units are presently estimated to be at 85% to 90% authorized strength.
6326 Morale is high, although replacements may not be highly trained.

6327 (2) Intelligence. Enemy stresses communications security and subordinate units of the 4th CAA
6328 have recently initiated intensive radio security and procedures training.

6329 (3) Operations.

6330 (a) Enemy is susceptible to mine warfare and antitank weapons.

6331 (b) Enemy has trained heavily on attack formations and has been told offensive action
6332 is the only way to victory.

6333 (c) Enemy is vulnerable to nuclear weapons due to massed forces and canalization by
6334 further advancement.

6335 (4) Logistics. Supplies are adequate for the enemy's conduct of either the offense or defense.
6336 The enemy had previously stockpiled supplies well forward in division areas.

6337 (5) Personalities. G/D Masonski, CG of the 10th MRD, is an advocate of penetration type
6338 offense on a narrow front with subsequent widening of the gaps to split enemy forces.

6339 4. ENEMY CAPABILITIES.

6340 a. Enumeration:

6341 (1) Attack at any time along sense of approach 1 with 4 motorized rifle battalions and 1 tank
6342 battalion supported by normal divisional and regimental artillery.

6343 (2) Attack at any time along avenue of approach 2 with 4 motorized rifle battalions and 1 tank
6344 battalion supported by normal divisional and regimental artillery.

6345 (3) Defend at any time with forces in contact supported by all available division and regimental
6346 artillery.

6347 (4) Reinforce his attack or defense with all or part of the following units at the places and times
6348 indicated:

<u>UNIT</u>	<u>PLACE</u>	<u>TIME</u>
(a) 30th MRR (-)	Avenue of approach 2	immediately
(b) 31st MRR (-)	Avenue of approach 1	immediately
(c) 37th TK Regt (-)	Avenue of approach 1	immediately
(d) 27th MRR (-)	Avenue of approach 1 or 2	2 hr after start of movement
(e) 23 MRR	vic LITTLE	8 hr after start of movement
(f) 121st TK Regt	Unlocated	Unknown
(g) U/I MRR of 19th MRD	vic BRAVO	9 hr after start of movement

6349 (5) Delay in successive positions to the east of LITTLE.

6350 (6) Employ chemical agents within our sector at any time.

6351 (7) Employ nuclear weapons of a 0.5-50 KT yield with delivery by artillery or SSM.

6352 (8) Employ guerrilla forces in our rear area either alone or in conjunction with the capabilities
6353 enumerated below.

6354

Figure A-2. Example format of an intelligence estimate (continued)

FOR OFFICIAL USE ONLY

6355 (9) The enemy can attack our area with an undetermined number of fighter, ground attack, and
 6356 bomb sorties daily. The maximum number of daily sorties mounted in our area has been 60.

6357 b. Analysis and Discussion.

6358 (1) Attack along avenue of approach 1.

6360 (a) The following indicate adoption of this capability:

6361 1 Uses a good avenue of approach.

6362 2 The enemy is massing motorized rifle elements, tanks, artillery and logistic
 6363 support along this avenue.

6364 3 Forward elements dispersed on a relatively narrow front.

6365 4 Extensive artillery preparation along approach.

6366 (b) The scant cover presented along this avenue of approach is a limiting factor but
 6367 does not preclude adoption of this capability.

6368 (2) Attack along avenue of approach 2.

6369 (a) The following indicate adoption of this capability:

6370 1 The enemy is massing mechanized elements, tanks, artillery and logistics
 6371 support along this avenue.

6372 2 Forward elements disposed on a relatively narrow front.

6373 3 Extensive artillery preparation along this avenue.

6374 (b) The following indicate rejection of this capability:

6375 1 This avenue of approach accommodates only one deployed regiment and
 6376 offers limited cover and concealment.

6377 2 The limited obstacle presented by GLENNVILLE.

6378 (3) Defend. The following indicate rejection of this capability:

6379 (a) The enemy is massing his forces along the line of contact.

6380 (b) Enemy has followed known doctrine for attack.

6381 (c) Terrain favors attack.

6382 (4) Reinforce. The following indicate adoption of this capability:

6383 (a) Movement of additional troops toward the front.

6384 (b) New units identified in the combat zone.

6385 (c) Forward logistical buildup.

6386 (5) Delay. There are no indications of the enemy's adoption of this capability.

6387 (6) Use chemical agents. There is no indication the enemy will employ chemical agents other
 6388 than smoke.

6389 (7) Use nuclear weapons. There is no indication the enemy will use nuclear weapons.

6390 (8) Use guerrilla forces. The following indicates adoption of this capability:

6391 (a) Doctrine calls for use of guerrilla force.

6392 (b) Use would enhance enemy advance by creating panic and confusion.

6393 (9) Air attack. Indications are the enemy will continue to use this capability as referenced in
 6394 paragraph (9) above.

6395 5. CONCLUSIONS.

6396 a. Intelligence. Available intelligence indicates that the division can accomplish its mission. Intelligence
 6397 support adoption of the division course of action.

6398 b. Weather and Terrain. The weather and terrain favors our defense. The best defensive area is the
 6399 high ground east of Dry Creek. The best avenue of approach into our defensive sector is avenue of
 6400 approach 1.

6401 c. Probable enemy courses of action.

6402 (1) Attack with forces in contact supported by air and artillery with the main attack of one
 6403 motorized rifle regiment along avenue of approach 1. Will reinforce with elements as indicated
 6404 in para 4a(4).

6405 (2) Conduct secondary attack with forces in contact supported by air and artillery with one
 6406 mechanized regiment along avenue of approach 2.

6407 (3) Employ guerrilla or special forces in our rear areas in conjunction with the above courses of
 6408 action.

6409 d. Enemy Vulnerabilities.

6410 (1) The Enemy is vulnerable to counterattack since he has been slow to exploit potential
 6411 penetrations.

6412 (2) Vulnerable to nuclear attack due to massing of troops and concentrated logistics depots.

6413

Figure A-2. Example format of an intelligence estimate (continued)

FOR OFFICIAL USE ONLY

6414
6415
6416
6417
6418
6419
6420
6421
6422
6423
6424
6425
6426

(3) Mine warfare will be effective against mechanized elements.
KROOK
BG

OFFICIAL:
/S/ Bagger
BAGGER
GS

Annex: A - Situation Overlay (omitted)
Distribution: A

6427

Figure A-2. Example format of an intelligence estimate (continued)

FOR OFFICIAL USE ONLY

**INTELLIGENCE RUNNING ESTIMATE
(CLASSIFICATION)**

Headquarters**Place****Date, time, and zone**

INTELLIGENCE RUNNING ESTIMATE NO. ____

References: Maps, charts, or other documents.

1. MISSION.

The unit's mission determined by the commander.

2. AREA OF OPERATION (IPB step 1).

State the unit's area of operation (AO) and established area of interest (AOI). Both physical and human geography must be taken into account. Consider tribal lines, family lines, cultural lines, economic lines, as well as physical lines such as roads and bodies of water. Cross-border ties may allow insurgents safe haven outside their country and aid in smuggling across the border. Information in this paragraph is based upon the facts and conclusions of intelligence preparation of the battlefield (IPB) and the analysis of the AO.

a. Terrain (IPB step 2).

(1) **Existing situation.** Terrain analysis observation and fields of fire, avenue of approach, key terrain, obstacles, concealment and cover [OAKOC]), analyzing the physical geography (natural and manmade features). In counterinsurgency (COIN) operations, emphasize complex terrain, suburban and urban terrain, key infrastructures, and lines of communication (LOCs). Complex terrain is multifaceted, with physical, social (human), and informational dimensions. Include as much information as necessary for an understanding of OAKOC. Geospatial engineer elements conduct a major portion of the terrain analysis. Geospatial overlay products include vegetation (tree spacing and trunk diameter), surface drainage (stream width, depth, velocity, bank slope, and height), surface materials (soil types and conditions that affect mobility), surface configuration (slopes that affect mobility), obstacles (natural and manmade—consider obstacles to flight as well as ground mobility), transportation systems (bridge classifications and road characteristics such as curve radius, slopes, and width), and effects of actual or projected weather such as heavy precipitation or snow cover.

Analyze the military aspects of terrain (OAKOC). **Observation and Fields of Fire:** Evaluating observation and fields of fire allow you to identify fire sacks and kill zones, ambush sites, engagement areas, battle positions, and defensible terrain. Identify specific system or equipment positions, and areas where maneuvering forces are most vulnerable to observation and fires. Include both visual or with the use of surveillance devices, include electronic and optical line of sight. Include friendly and enemy systems such as weapon sights, laser range finders, radars, radios, and jammers. Identify observation posts and listening posts, areas of visual dead space. **Avenues of Approach:** An air or ground route of an attacking force of a given size leading to its objective or to key terrain in its path. Include air and ground routes (and mobility corridors), to assist in development of named areas of interest (NAIs) and target areas of interest (TAIs), infiltration routes, and exfiltration routes; **Key Terrain:** For enemy and friendly units—tall structures, choke points, intersections, bridges, industrial complexes.

FOR OFFICIAL USE ONLY

In COIN, the people of the area are always key terrain. **Obstacles:** Manmade or natural terrain that stop, impede, or divert military movement. Examples include cant and slope, intervening crests, rivers, lakes, forests, deserts, swamps, jungles, built-up areas, densely populated areas, buildings, road craters, minefields, and trenches. Obstacles to air mobility include features that exceed the aircraft's service ceiling restrict nap-of-the-earth flight or that force the aircraft to employ a particular flight profile, and obstacles that affect the aircraft landing zone and drop zone. Examples are tall trees, towers, power lines, buildings, rapidly rising terrain features, mountains, and smoke or other obscurants. **Cover and Concealment:** Cover examples from direct and indirect fires include ditches, caves, river banks, folds in the ground, ridges, fingers, forested and built-up areas, shell craters, buildings, walls, and embankments. Concealment examples include woods, underbrush, snowdrifts, tall grass, and cultivated vegetation. The evaluation of cover and concealment aids in identifying defensible terrain, possible approach routes, assembly areas, deployment and dispersal areas, ambush sites or positions, specific system or equipment locations, and battle positions.

Use graphic representations and overlays. Use annexes for detailed material. Include effects of chemical, biological, radiological, nuclear, and high-yield explosives (CBRNE) and enhanced conventional weapons fires, and any other pertinent considerations on each of these factors as appropriate.

(2) **Effect on enemy operations and broad COAs.** Describe the effects of terrain on enemy operations and broad COAs. State how it favors or disfavors enemy operations. Include how the terrain affects the threat's use of CBRNE weapons, and any special methods, techniques, equipment, procedures, or forces the threat may have.

(3) **Effect on own operations and broad COAs.** Describe in the same manner as for (2) above, except exclude the friendly use of biological agents.

b. Civil Considerations.

(1) **Existing situation.** Civil Considerations (ASCOPE) are analyzed for all types of military operations. Civil considerations of the environment can either help or hinder friendly personnel and mission, as well as the threat's personnel and mission. Understanding the impact on military operations better prepares the commander and staff, and enhances situational awareness and situational understanding. Analyze civil considerations using the acronym ASCOPE: Areas, Structures, Capabilities, Organizations, People, Events. Use templates and overlays to graphically depict civil considerations areas analyzed.

(a) **Areas.** Analyze the localities and aspects of the terrain that are not normally militarily significant to determine key civilian areas. Analyze the key civilian areas to determine how military operations affect these areas, and how these areas affect military operations. Examples of key civilian areas are (1) Boundaries, (for example, political precincts and districts, districts within a city, or municipalities within a region; boundaries for social, religious, or criminal enclaves; (2) Government centers; (3) Commercial zones (for example, agricultural regions, mining regions, trade routes; (4) LOCs (for example, street patterns, urban patterns, subterranean passages and underlying terrain; and (5) Possible sites for military applications (for example, temporary settlement of displaced civilian camps or other civil functions).

(b) **Structures.** Structures include (1) high-value targets (HVTs) or HPTs (for example, bridges, communication towers, power plants, dams; (2) cultural sites protected by international law or other agreement (for example, churches, temples, mosques, national libraries, and hospitals; (3) Structures that have practical applications which can support military operations (for example, jails, warehouses, television and radio stations, and print plants).

FOR OFFICIAL USE ONLY

(c) **Capabilities.** Host nation (HN), aggressor nation or some other body's ability to provide key functions or services to save, sustain, or enhance life (in that priority). Examples include emergency services, fire and rescue, food, water supply, fuel, electric power stations, communication facilities, health services, public works and utilities, public safety, public health, public administration, economics, commerce, and technology. Also include resources and services that can be contracted to support the military. Examples include interpreters, laundry services, construction materials, and equipment.

(d) **Organizations.** Non-military groups or institutions in the AO that interact and influence with the populace and the force. Indigenous examples include church groups, fraternal organizations, patriotic or service organizations, labor unions, criminal organizations, and community watch groups. Groups from outside the area include corporations, United Nations agencies, US governmental agencies, and NGOs, such as the International Red Cross/Red Crescent. Include information on their activities, capabilities, and limitations, how their activities affect military operations, and vice versa.

(e) **People.** Civilians within or outside the AO whose actions, opinions, or influence can affect the mission, either positively, negatively, or neutrally. Analyze and identify by their capabilities, needs, and intentions. Consider historical, cultural, ethnic, political, economic, humanitarian factors, key communicators, formal and informal influences. Examples to include are history of the area and how it influences the insurgency, events leading or contributing to the insurgency; tribal, clan, or familial groups and their geographic location and their influences; religious groups, their geographic location, and their influences; ethnic groups, their geographic location and their influences; languages spoken; key people who influence the society, their affiliations and loyalties, and their interrelations with other people; public perceptions of the insurgency; points of agreement or disagreement with insurgent ideology or ideologies; major industries and sources of employment; communication links to other regions; and media influence on local populace.

(f) **Events.** Events are routine, cyclical, planned, or spontaneous activities that significantly affect people, organizations, or military operations. Examples include national and religious holidays, agricultural crop or livestock and market cycles, elections, civil disturbances, and celebrations. Examples of spontaneous events include disasters from natural, manmade, or technological sources. These events create civil hardship and require emergency responses. Also include events precipitated by military forces. Examples include combat operations, deployments, redeployments, and paydays. Once significant events are determined, template and analyze the events for their political, economic, psychological, environmental, and legal implications.

(2) **Effect on enemy operations and broad COAs.** Describe the civil considerations effects on enemy operations and broad COAs. State how it favors or disfavors enemy operations. Also include how the threat's use of CBRNE weapons and any special methods, techniques, equipment, procedures, or forces the threat employees affects civil considerations, and vice versa. Use templates and overlays.

(3) **Effect on own operations and broad COAs.** Describe in the same manner as for (2) above, except exclude the friendly use of biological agents.

c. Weather.

(1) **Existing situation.** The main portion of weather analysis is conducted by the Air Force Staff Weather Officer (SWO). Using geospatial intelligence (GEOINT) principles and techniques, the engineer detachment works closely with the SWO to ensure the terrain analysis incorporates the effects of current and projected weather, thus enhancing automated support of the terrain analysis process.

FOR OFFICIAL USE ONLY

Include climate, current weather report, and weather forecasts on the overall environment. Evaluation of the military aspect of weather include visibility, winds, precipitation, cloud cover, temperature, and humidity. The analysis focus is on the effects of weather on military operations rather than on the factors that make up the analysis. Include thermal crossover, a natural phenomenon which normally occurs twice daily when temperature conditions are such that there is a loss of thermal contrast between two adjacent objects. Include light data for the period of time of military operations. Use appendixes for detailed information.

(2) **Effects on METT-TC.** Describe how the weather favors or disfavors mission, enemy, terrain and weather, troops and support available, time available, and civil considerations (METT-TC).

d. Other Characteristics. When applicable, include other characteristics not covered above. Analyze using the same subheadings (existing situation, effect on enemy operations, effect on own operations and COA). Examples of other characteristics may include wildlife or diseases.

3. ENEMY SITUATION.

This paragraph gives information on the enemy, which will permit later development of their capabilities and vulnerabilities, and refinement of these capabilities into specific COAs and their relative probability of adoption.

a. Composition.

In conventional operations: Summary of threat characteristics that can influence accomplishment of the mission. Include state and unit organization. Special mention is made of electronic warfare (EW), special operations forces (SOF), and CBRNE, as appropriate. **In COIN operations:** Key influential people; political cadre, cells, organization; C2 staff (internal and external), intelligence cells, attack teams and operation cells, finance (internal and external), logistic and support cells, external ties; and, as required, religious organization; ethnic organization; tribal organization; and family organization. Special mention is made of EW, SOF, and CBRN, as appropriate. Reference other documents, as required.

b. Disposition.

In conventional operations: Geographic location of threat elements and how they are deployed or employed. Include recent, current, and projected movements. Reference overlays, situation maps (SITMAPs), previously published documents. **In COIN operations:** Areas of control (religious, ethnic, tribal, political, and/or familial demographics and neighborhoods), C2 locations, safe houses, front organizations, training camps, and sustainment and support locations.

c. Strength.

In conventional operations: Committed forces, reinforcements, air, and CBRNE weapons. The preponderance of strength or lack thereof affects the raising or lowering of the analyst's estimate of the enemy capabilities and vulnerabilities in paragraph 5. Information concerning strength provides an indication of threat capabilities and helps determine the enemy probable COAs or options open or closed.

(1) **Committed Forces.** Include ground maneuver units currently in contact and those ground maneuver units with which imminent contact can be expected, regardless of the specific friendly COA, location, controlling headquarters, and doctrine. The intelligence officer usually accounts for committed forces based upon the size of unit doctrinally used to oppose the friendly unit. Generally, enemy units are

FOR OFFICIAL USE ONLY

counted in terms of units two echelons below the friendly unit's size. (For example, a brigade S-2 normally considers committed forces in terms of companies; a division G-2 in terms of battalions; and a corps G-2 in terms of regiments or brigades.) If there is doubt whether a unit is a committed force or a reinforcement, it is considered a reinforcement. This attributes to the enemy the maximum capability to reinforce forces to oppose a given friendly COA.

(2) **Reinforcements.** Include designation and location. Reinforcements are those enemy maneuver units that may or may not be employed against friendly forces, depending upon our specific choice of a COA and upon enemy plans. Reinforcements are enemy units not committed in or out of the friendly sector, but which can react to the friendly COA, subject to time and distance considerations, in time to influence the accomplishment of the mission. Imminent contact is not expected. Disposition, location, level of control, or other factors at the time of the estimate are considered in determining which enemy forces are reinforcements.

(3) **Air.** List the number of enemy aircraft by type within operational radius; if known, include the number of possible sorties per day by type of aircraft.

(4) **CBRNE Weapons and Agents.** Estimate, as appropriate, the number, type, yield, and the delivery means of enemy CBRNE weapons or agents available to the enemy.

In COIN operations: Generating popular support is the center of gravity of the insurgency. Insurgent strength is measured largely by how much popular support the insurgency has. As the insurgent group gains in support, its capabilities grow, which in turn enable it to gain more support. Popular support results in safe havens, freedom of movement, logistical support, financial support, intelligence, and new personnel for the insurgency. A gain in support for the insurgents is a loss for the government, and a loss of support for the government is a gain for the insurgents. Evaluate and list the following:

(a) Level of popular support to the insurgency relative to the government includes regional, national, international support. Popular support can range from sympathizers to assistance in conducting operations, storage or moving sustainment, or just withholding information. Include information on the areas they control (religious, ethnic, tribal, political organization, demographics, and neighborhoods).

(b) Forms of popular support the insurgents receive may include safe havens, freedom of movement, logistical support, financial support (internal and external), intelligence, and recruitment for the threat.

(c) Sources of popular support by type (active, passive, internal, external).

(d) Segments of populace supporting the insurgency.

(e) Foreign government support may come from a variety of venues; for example, influential figures pronouncing support; training facilities or safe houses; recruitment, financial support; and providing safe passage across national or international borders. The insurgency may also receive sustainment from national and international countries.

(f) NGO support.

(g) Criminal network support.

(h) Other sources of support.

(i) Methods used to generate popular support and their effectiveness.

(j) Grievance (real or perceived) exploited by insurgents.

(k) Capabilities and vulnerabilities in generating popular support.

FOR OFFICIAL USE ONLY

(l) Attack teams and operation cells.

(m) Recruitment.

d. Tactics and Training. In conventional and COIN operations list strategy, methods of operations, and doctrine, tactics, and training or other information of interest that provide a basis for analysis to determine relative probability of adoption of specific COAs and to determine enemy vulnerabilities. Enemy failure to take expected action is listed, as well as positive information. In COIN operations, tactics also involve political, military, psychological, and economic considerations. Tactics may include assassinations, arson, bombings, hostage taking, kidnapping, hijacking, seizure, raids, sabotage, denial and deception, hoaxes; use technology to destroy key elements of the national infrastructure—transportation, telecommunications, energy, banking, public health, and water supply; and use CBRNE.

e. Sustainment. Analysts can more accurately evaluate the enemy capabilities, strengths, and combat effectiveness. With knowledge of the enemy's sustainment and support structure. The enemy's adoption of a COA depends on the logistical system to support the action. In conventional operations include procurement, maintenance, distribution, and replacement of all types of material including transport of personnel. In COIN operations, sustainment may include weapons and ammunition, IED and bomb-making components, food, water, propaganda equipment and materials, medical, transportation, and finance. Finance is who is providing the threat with financial support, how the money is transferred, and which financial institutions the enemy uses.

f. Operational Effectiveness. Operational effectiveness studies the threat morale, weapons effectiveness, equipment readiness, leadership, and personnel. Strength must be tied to the operational effectiveness, but is important enough to have its own mention earlier in the estimate. Conventional weapons, such as artillery ranges, should be addressed here.

g. Intelligence. Estimate the enemy's intelligence collection capability. Include how threat picks and evaluates a target; method of ISR; ISR success, ISR vulnerabilities, or ISR susceptibility to deception and detection. HUMINT, IMINT (including threat use of commercial software) and EW capabilities must be addressed if known. How the threat passes intelligence information—radio, cell phone, electronic message—and how it can be interdicted.

h. Communications. Evaluate and list enemy's communication modes may include high-frequency short wave, cell phone, Internet, mail, courier, face-to-face, Citizen Band, or Amateur radio sets or the drop system.

i. Other. Use the threat characteristics listed in chapter 3 and include any other factors necessary for creating as thorough a picture of the threat as possible.

4. ENEMY CAPABILITIES.

Based upon all the previous information and analyses, develop and list enemy capabilities and limitations. A capabilities listing provides a basis for analyzing the available information. It shows those capabilities the enemy can adopt as specific COAs and their relative probability of adoption.

In COIN operations: The listing should show the task and purpose.

In conventional operations:

a. State enemy's capabilities. State what, where, when, and in what strength for each capability.

b. State enemy's limitations. Discuss each limitation, the cause and effect.

FOR OFFICIAL USE ONLY

Figure A-3. Example of an intelligence running estimate format (continued)

c. Analysis and Discussion. Discuss each capability (or appropriate combination of capabilities) in a separate subparagraph, and any effects of the terrain, civil considerations, and/or weather may have on each capability. This will provide a basis for conclusions of enemy capabilities and their relative probability of adoption. Include consideration of enemy deception measures. All the previous pertinent information and conclusions are tabulated as either supporting or rejecting the adoption of the capability. After listing all the evidence, each capability is judged from the point of view of whether the adoption of the capability is advantageous to the enemy. Such judgments need not be made if the conclusion is obvious, or if there is no evidence that the enemy will adopt the capability, unless the capability is one that will make the accomplishment of the friendly mission highly doubtful or impossible. This exception is to focus attention on dangerous threats.

In COIN operations. Evaluation of the threat in COIN operations must begin early and cover a wide range of factors in building an accurate threat model. Based upon all the information and analysis, develop and list enemy capabilities. First, evaluate the following characteristics of the insurgency as a basis for evaluating the enemy COA.

a. Insurgent goals. Does the threat desire a different social or political organization than that which exists under current conditions? How will they conduct operations towards that goal?

b. Insurgent motivations. Are they motivated by ideological, religious, or monetary?

c. Popular support. Include regional, national, and international.

d. Key leaders and personalities. Key influential people, political, ideological, religious, military, and key members who bring expertise (demolition special weapons, assassinations, specialized trainers) staff members, family members, and informal leaders.

e. Organization.

f. Morale of the leaders and members.

g. Then, evaluate the enemy's capability to conduct operations. This should tie in with Operational Effectiveness (paragraph 3f above). State each capability as a task and purpose. State what, where, when, and in what strength for each task. State enemy's limitations and vulnerabilities. Include the cause and effect of the limitation. Evaluate the following capabilities of the insurgency as a basis for evaluating the threat COA:

(1) Conduct violent activities (for example, murder, assassination, arson, bombing, hostage taking, kidnapping, hijacking, seizure, and raids).

(2) Conduct other operations (for example, sabotage, denial and deception, hoaxes, and use of technology).

(3) Conduct intelligence operations.

(4) Conduct training.

(5) Conduct sustainment and supply activities.

(6) Conduct information activities.

(7) Conduct political activities.

(8) Conduct recruitment.

h. Analysis and Discussion. Discuss each capability (or appropriate combination of capabilities). In a separate subparagraph, include any effects of the terrain, civil considerations, and/or weather may have on

FOR OFFICIAL USE ONLY

each capability. This will provide a basis for conclusions of enemy capabilities and their relative probability of adoption. Include consideration of enemy deception measures. All the previous pertinent information and conclusions are tabulated as either supporting or rejecting the adoption of the capability. After listing all the evidence, each capability is judged from the point of view of whether the adoption of the capability is advantageous to the enemy. Such judgments need not be made if the conclusion is obvious, or if there is no evidence that the enemy will adopt the capability, unless the capability is one that will make the accomplishment of the friendly mission highly doubtful or impossible. This exception is to focus attention on dangerous threats.

5. CONCLUSIONS.

Based upon all the previous information and analysis, state conclusions concerning the total effects of the AO on threat operations. List all the possible threat COAs in the order of probability of adoption. Include threat vulnerabilities that can be exploited. State which COAs are considered most likely and those that are the most dangerous COAs. This will assist the commander and staff in selecting friendly COA during wargaming.

a. Probable threat COAs. List COAs in order of relative probability of adoption. A listed COA may include several subordinate COAs that can be executed concurrently. Usually, no more than two or three COAs, in order of probability of adoption, can be justified by the available evidence. The G-2/S-2 should identify which COA is most likely and which is most dangerous at a minimum.

b. Threat vulnerabilities. List the threat peculiarities and weaknesses that result in vulnerabilities which are exploitable at own, higher, or lower levels of command.

c. Intelligence consideration on operations. Indicate whether the mission set forth in paragraph 1 above can be supported from the intelligence standpoint. Indicate which COAs can best be supported.

/s/ _____

(Designation of staff officer)

(CLASSIFICATION)

FOR OFFICIAL USE ONLY

Figure A-3. Example of an intelligence running estimate format (continued)

FINAL DRAFT

FOR OFFICIAL USE ONLY

6440

Appendix B

6441

Language Support

6442

ROLE OF LINGUISTS

6443

B-1. Military operations are highly dependent on military and contractor-provided foreign language support. The requirement to communicate with and serve on multinational staffs, communicate with local populations, and exploit enemy forces necessitates the use of linguists. The growing focus on multinational operations increases the competition for limited linguist resources that are vital for mission success. This appendix establishes the framework and process to access, prioritize, and employ the Army's limited organic linguist resources.

6444

6445

6446

6447

6448

6449

LINGUISTIC SUPPORT CATEGORIES

6450

B-2. Foreign language support requirements of US Armed Forces typically fall into one of four broad categories:

6451

6452

- **Intelligence and Information Collection.** This category includes the traditional SIGINT and HUMINT disciplines, as well as foreign language support to protection and exploitation of open-source information.

6453

6454

6455

- **Operations and Multinational Liaison.** This category includes the coordination of military operations and liaison with multinational partners, previously unaffiliated nations, and at times adversary or former adversary nations. Multinational operations are becoming more common and increasingly important.

6456

6457

6458

6459

- **Civil Affairs Activities.** CA activities enhance the relationship between civil authorities in areas with military forces. They involve applying CA functional specialty skills to areas normally under the responsibility of civil government. These operations involve establishing, maintaining, influencing, or exploiting relations between military forces and all levels of HN government agencies. These activities are fundamental to executing stability tasks. CA personnel, other Army forces, other government agencies, or a combination of all three perform these tasks. Foreign language support is critical to CA in areas such as government liaison, legal agreements, medical support and operations, law enforcement, engineering projects, public safety, security and population control, and PSYOP.

6460

6461

6462

6463

6464

6465

6466

6467

6468

- **Sustainment.** This category consists of foreign language support to sustainment functions. These functions include logistical contracting, port, railhead, airhead, or transshipment operations and convoy operations.

6469

6470

6471

DETERMINING LINGUIST REQUIREMENTS

6472

B-3. To identify linguist requirements, the staff conducts mission analysis and identifies specified or implied tasks requiring foreign language support. Other critical factors are the organization or echelon of command and the location of the mission. The staff uses these criteria to determine the allocation of linguists, such as one linguist team per echelon of command, one linguist per piece of equipment, or one linguist team per location where the function is to be performed. The staff then applies METT-TC to determine the number of linguists needed for an operation.

6473

6474

6475

6476

6477

6478

B-4. The staff must analyze each linguist assignment to determine the minimum level of foreign language proficiency needed. While interpretation for a peace negotiation requires not only outstanding linguistic capability but also cultural acumen, the translation of routine documents (with the aid of a dictionary)

6479

6480

FOR OFFICIAL USE ONLY

6481 requires a much different skill set. Poor identification of linguist proficiency requirements can tie up the
6482 best linguists in less effective roles, creating linguist shortfalls in other areas.

6483 B-5. The relative importance of each of the four linguist support categories is mission dependent. For
6484 example, during a noncombatant evacuation operation civil and military coordination would probably not
6485 be as critical as intelligence and information collection. However, the situation is reversed for stability
6486 missions. Identifying these “dynamics” helps the commander and staff prioritize linguist requirements.

6487 B-6. Determining linguist requirements for any operation can be difficult because each operation is
6488 unique. However, commanders and staffs with a basic knowledge of organic Army linguistic assets,
6489 foreign language resource alternatives, and MI skills can successfully assess, prioritize, and employ
6490 linguists in support of their military operations.

6491 **PLANNING AND MANAGING LINGUIST SUPPORT**

6492 B-7. Commanders must consider the linguist requirements as part of their MDMP for every contingency
6493 plan and OPLAN assigned to their commands. Prior staff planning and identification of linguist
6494 requirements should prompt commanders to initiate linguist support requests and identify command
6495 relationships prior to actual operations.

6496 B-8. If the mission analysis reveals requirements for linguistic support, the commander must identify what
6497 foreign languages are needed, the foreign language proficiency levels needed for each assignment, and the
6498 best source of linguists. In addition, if the mission includes intelligence and information collection, the
6499 commander must identify MI collection skills required. During mission analysis, commanders should
6500 consider linguist requirements for every contingency plan and OPLAN assigned to their command.

6501 **LINGUIST CATEGORIES**

6502 B-9. The commander and staff must identify linguist requirements by category:

- 6503 • **Category I** – Have native proficiency in the target language (level 4-5) and an advanced
6504 working proficiency (Interagency Language Round Table [ILRT] level 2+) in English. They
6505 may be locally hired or from a region outside the AO. They do not require a security clearance.
6506 They must be screened by the Army CI support team.
- 6507 • **Category II** – Are US citizens screened by Army CI personnel and are granted access to
6508 SECRET by the designated US Government personnel security authority. Have native
6509 proficiency in the target language (level 4-5) and an advanced working proficiency (ILRT 2+) in
6510 English.
- 6511 • **Category III** – Are US citizens screened by Army CI personnel and are granted either TS/SCI
6512 clearance or an interim TS/SCI clearance by the designated US government personnel security
6513 authority. Meet a minimum requirement of ILRT 3. They are capable of understanding the
6514 essentials of all speech in a standard dialect. They must be able to follow accurately the
6515 essentials of conversation, make and answer phone calls, understand radio broadcasts and news
6516 stories, and oral reports (both of a technical and non-technical nature).

6517 **PRIMARY STAFF RESPONSIBILITIES**

6518 B-10. Primary staff at each echelon has responsibilities for evaluating requirements and managing linguist
6519 support. The responsibilities include but are not limited to those discussed below. In addition, each staff
6520 section is responsible for determining its linguist support required to meet its operational missions.

6521 **ASSISTANT CHIEF OF STAFF, G-1 (S-1):**

- 6522 • Identify linguist requirements needed to support G-1/S-1 functions in all contingency areas.
6523 G-1/S-1 requirements for linguist support include but are not limited to the following:

FOR OFFICIAL USE ONLY

-
- 6524 ■ Coordinate with local authorities on matters of civilian hire, financial management, and recordkeeping.
 - 6525
 - 6526 ■ Coordinate for local morale support and community activities.
 - 6527 ■ Coordinate with local authorities for postal operations.
 - 6528 ■ Support for administration, counseling, personal affairs, and leave for local national and third-country national personnel.
 - 6529
 - 6530 ■ Liaison with multinational counterparts.
 - 6531 ● Linguist staffing and linguist replacement management.
 - 6532 ● Identify foreign language skill identifiers for all assigned, attached, or OPCON Army linguists.
 - 6533 ● Identify all Army foreign language skilled Soldiers not identified on electronic Military Personnel Office System or the Defense Integrated Military Human Resource System (DIMHRS).
 - 6534
 - 6535
 - 6536 ● Deploy and provide human resource support to DA and DOD civilian linguists.
 - 6537 ● Provide human resource support for LN linguists.
 - 6538 ● Procure Army foreign language support personnel for screening local labor resources.

6539 **ASSISTANT CHIEF OF STAFF, G-2 (S-2):**

- 6540 ● Identify linguist requirements needed to support G-2/S-2 functions in all contingency areas. G-2/S-2 requirements for linguist support include but are not limited to—
- 6541 ■ Identifying Category II and Category III linguist requirements.
- 6542 ■ Evaluating and/or using local maps and terrain products in operations.
- 6543 ■ Processing for MI purposes material taken from detainees or civilian internees.
- 6544 ■ At lower echelons, conducting Soldier surveillance and reconnaissance.
- 6545 ■ Assessing local open-source information for intelligence value.
- 6546 ■ Coordinating intelligence and liaison with multinational and HN counterpart.
- 6547
- 6548 ● Determine, during the initial IPB, all foreign languages (spoken and written) and dialects needed for mission accomplishment.
- 6549
- 6550 ● Collect, process, produce, and disseminate information derived from linguist sources.
- 6551 ● Provide intelligence training for MI linguists employed in AOs.
- 6552 ● Coordinate for security investigations, as necessary, for local hire linguists.
- 6553 ● Provide support to CI screening of contracted linguists and LN labor force.

6554 **ASSISTANT CHIEF OF STAFF, G-3 (S-3):**

- 6555 ● Identify linguist requirements needed to support G-3/S-3 functions in all contingency areas. G-3/S-3 requirements for linguist support include but are not limited to—
- 6556 ■ Identify CAT II and CAT III linguist requirements.
- 6557 ■ Operational coordination and liaison with multinational and HN counterparts.
- 6558 ■ Translate OPODs and OPLANs for use by multinational counterparts.
- 6559
- 6560 ● Consolidate unit linguistic requirements and establish priorities.
- 6561 ● Develop linguist deployment and employment plans.
- 6562 ● Develop plans to train linguists and to use linguists for training the force in AO's foreign language survival skills. In addition to global language skills, linguists must have training in specific vocabulary used in the AO; for example, terms used for military, paramilitary, civilian or terrorist organizations, and ethnic groups within the area, nomenclatures of equipment used, and other military or technical vocabulary. Training in the specific dialect used in the AO would also be beneficial.
- 6563
- 6564
- 6565
- 6566
- 6567
- 6568 ● Assign, attach, and detach linguists and linguist teams.

FOR OFFICIAL USE ONLY

- 6569 ● Integrate additional or replacement linguists through operational channels.
- 6570 ● Recommend modernization and development of linguist systems and methods.
- 6571 ● Coordinate mobilization and demobilization of USAR and USARNG linguist support.
- 6572 ● Plan linguist usage for deception operations.
- 6573 ● Plan linguist support for movement of EPWs, detainees, and displaced civilians.
- 6574 ● Coordinate evaluation of linguist support by all staff elements.

6575 **ASSISTANT CHIEF OF STAFF, G-4 (S-4):**

- 6576 ● Identify linguist requirements needed to support G-4/S-4 functions in all contingency areas.
- 6577 G-4/S-4 linguist requirements for linguist support include but are not limited to—
 - 6578 ■ Procure local supply, maintenance, transportation, and services.
 - 6579 ■ Coordinate logistics at air and seaports of debarkation.
 - 6580 ■ Contract with local governments, agencies, and individuals for sites and storage.
 - 6581 ■ Contract for and hire local personnel.
- 6582 ● Provide logistical, supply, maintenance, and transportation support to attached linguists.

6583 **ASSISTANT CHIEF OF STAFF, G-6 (S-6):**

- 6584 ● Identify linguist requirements needed to support G-6/S-6 functions in all contingency areas.
- 6585 G-6/S-6 linguist requirements for linguist support include but are not limited to—
 - 6586 ■ Coordinate suitable commercial information systems and services.
 - 6587 ■ Coordinate with multinational forces on command frequency lists.
 - 6588 ■ Coordinate signal support interfaces with HN and multinational forces.
- 6589 ● Manage RF assignments for supporting linguist elements.
- 6590 ● Support linguist operations with internal document reproduction, distribution, and message
- 6591 services.
- 6592 ● Integrate automation management systems of linguist units.

6593 **ASSISTANT CHIEF OF STAFF, G-7 (S-7):**

- 6594 ● Foster and support mutually planned and synchronized PSYOP and information operations
- 6595 efforts.

6596 **ASSISTANT CHIEF OF STAFF, G-9 (S-9):**

- 6597 ● Identify linguist requirements needed to support G-9/S-9 functions in all contingency areas.
- 6598 G-9/S-9 linguist requirements for linguist support include but are not limited to—
 - 6599 ■ Determine civilian impact on military operations.
 - 6600 ■ Minimize civilian interference with operations.
 - 6601 ■ Recommend curfews, movement restrictions, and relocations if applicable.
 - 6602 ■ Provide assistance to liaison with HN and multinational agencies, dignitaries, and
 - 6603 authorities.
 - 6604 ■ Promote positive community programs to win over support.
 - 6605 ■ Determine if multinational operations PSYOP efforts are mutually planned and
 - 6606 synchronized.
 - 6607 ■ Support, as necessary (to include interpreters) resolution of civilian claims against the US
 - 6608 Government.
 - 6609 ■ Protect culturally significant sites through command recommendations.
 - 6610 ■ Use linguistic and cultural support to identify cultural and religious customs.

FOR OFFICIAL USE ONLY

-
- 6611 • Assist the G-1 in the administrative support to identify linguists and G-4 in the contracting of
6612 local hires (especially linguists).
6613 • Identify foreign language requirements to support stability operations.
6614 • Identify and adjust use of HN and other resources (such as linguists and labor) available from
6615 civil authorities.

6616 **SPECIAL STAFF OFFICER RESPONSIBILITIES**

6617 B-11. Linguist requirements for special staff officers include but are not limited to the staff officers shown
6618 in table B-1.

FOR OFFICIAL USE ONLY

Table B-1. Special staff officer responsibilities

SPECIAL STAFF OFFICER	RESPONSIBILITIES
Liaison Officers	<ul style="list-style-type: none"> • Should speak the required foreign language. If not, they require a translator or interpreter for all aspects of their duties. • Request interpreters to assist when representing the multinational operations. • Translate orders, maps, traces, overlays, and documents into multinational foreign languages.
Civilian Personnel Officers	<ul style="list-style-type: none"> • Recruit, interview for suitability, and hire civilian local labor force if required. • Negotiate host country on labor agreements.
Dental Surgeon	<ul style="list-style-type: none"> • Administers dental care to support humanitarian mission requirements. • Rehabilitates, constructs, and gains access to existing dental facilities as required.
Financial Management Officer	<ul style="list-style-type: none"> • Supports the procurement process of local goods and services not readily available through normal logistical channels. • Ensures limited non-US and US pay functions to foreign national, HN, civilian internees, and detainees are provided. • Ensures all necessary banking functions are performed in theater.
Surgeon	<ul style="list-style-type: none"> • Supports medical humanitarian assistance and disaster relief operations. • Provides medical care of detainees and civilians within the command's AO. • Coordinates medical laboratory access in AO. • Determines the nature of local health threats to the force through populace interviews. • Determines the identity of local or captured medical supplies.
Veterinary Officer	<ul style="list-style-type: none"> • Determines source and suitability of local foods. • Assists the local population with veterinary service needs.
Chemical Officer	<ul style="list-style-type: none"> • Identifies enemy force chemical weapons and equipment. • Communicates CBRNE risks to supported populations.
Engineer Coordinator	<ul style="list-style-type: none"> • Procures proper local materials to support engineering missions. • Communicates engineering project requirements to contracted local work force. • Communicates engineering project impact on local landowners and other affected parties. • Determines, in coordination with G-2/S-2, suitability of local topographic maps and terrain products. • Assesses environmental concerns of HN and local populations in combined operations.
Provost Marshal	<ul style="list-style-type: none"> • Supports displaced civilian control activities. • Supports internment and resettlement operations, to include displaced civilians. • Supports weapons buy-back programs, as required, and works closely with civil-military liaisons for payments to local officials. • Supports counter-drug and customs activities. • When authorized, helps foreign civil authorities maintain control. • Conducts liaison with local LEAs.
PSYOP Officer	<ul style="list-style-type: none"> • Produces approved PSYOP propaganda and counter-propaganda media. • Evaluates PSYOP impact on target audience.

FOR OFFICIAL USE ONLY

6620

Table B-1. Special staff officer responsibilities (continued)

SPECIAL STAFF OFFICER	RESPONSIBILITIES
Air Defense Coordinator	<ul style="list-style-type: none"> • Supports identification of enemy air defense artillery. • Communicates air defense warnings to supported populations. • Communicates air defense project requirements to contracted local work force.
Safety Officer	<ul style="list-style-type: none"> • Provides safety training to local labor force. • Communicates warnings of dangerous military operations and other hazards to local populace.
Transportation Officer	<ul style="list-style-type: none"> • Coordinates commercial and local transportation needs. • Coordinates movement scheduling and routes with multinational forces and/or HN.
Surgeon	<ul style="list-style-type: none"> • Determines the nature of local environmental health threat to the force through populace interviews.

6621 **PERSONAL STAFF OFFICER RESPONSIBILITIES**

6622 B-12. Linguist requirements for special staff officers include but are not limited to the staff officers shown
6623 in table B-2.

Table B-2. Personal staff officer responsibilities

PERSONAL STAFF OFFICER	RESPONSIBILITIES
Chaplain	<ul style="list-style-type: none"> • Coordinates religious support with multinational partners. • Determines the impact of local population religious group faiths and practices on military operations. • Provides religious support to the community to include hospital patients, detainees, displaced civilians, and civilian detainees. • Conducts liaison with local population religious leaders in close coordination with the G-9.
Public Affairs Officer	<ul style="list-style-type: none"> • Acts as the commander's spokesman for all communication with external media. • Assesses the accuracy of foreign media interpretation of Public Affairs Office (PAO) releases. • Assesses and recommends news, entertainment, and other information (assisting G-9) for contracted services foreign nationals.
Staff Judge Advocate	<ul style="list-style-type: none"> • Translate and interpret foreign legal codes, SOFAs, and international laws. • Determines local environmental laws and treaties through translation services. • Assesses the treatment of detainees and civilian internees. • Translates documents to support G-4 in local contracts.

6624 **SOURCES OF LINGUISTS**

6625 B-13. There are various sources that a commander can use to obtain the linguists necessary to support
6626 operations. It is vital to know the advantages and disadvantages of each type of linguist and to carefully
6627 match the available linguists to the various aspects of the operation.

FOR OFFICIAL USE ONLY

6628 **ARMY LANGUAGE-QUALIFIED MOS/AOCs**

6629 B-14. The MI language-dependent enlisted MOSs are 35P with an SQI of L (Cryptologic Communications
6630 Interceptor/Locator) and 35M (HUMINT Collector) and their related WO AOC of 352P and 351M. Some
6631 Soldiers in MOS 35F (All-Source Intelligence Analyst), MOS 35L (CI Agent), and MOS 35N (SIGINT
6632 Analyst), and their related WO AOCs 350F, 351L, and 352N are trained in foreign languages.

6633 B-15. Utilizing Soldiers in the MOSs and AOCs mentioned above has many advantages. They are already
6634 trained in the military system, are not subject to deployment restrictions (a limiting factor with civilian
6635 linguists), have a security clearance and, as US personnel, support the command's interests. The major
6636 disadvantage to utilizing these individuals for general foreign language support is that in doing so, they are
6637 removed from their primary MI functions. They should be used only in linguistic duties that include
6638 intelligence potential.

6639 B-16. Non-MI Army language-qualified enlisted MOSs and officer AOCs are in career management
6640 fields/branch codes 18 (Special Forces [enlisted and officers]), 37 (PSYOP), 38 (CA), 180A (Special
6641 Forces WO); and functional area 48 (Foreign Area Officer). Particular attention must be paid to the
6642 recorded language proficiency and test date of these individuals since the standards vary by field. The same
6643 advantages and disadvantages apply as with the MI linguists.

6644 B-17. The Army also includes linguists in MOS 09L (translator/interpreter). The 09Ls are specifically
6645 trained to be a translator and interpreter. They have the same advantages as listed above for language-
6646 dependent MOS/AOCs. An added advantage is that since their sole job is translation and interpretation,
6647 they do not have to be removed from another job in order to be used as a linguist. Their major disadvantage
6648 is that they have no additional skill that gives them dual functionality as do the 18, 37, 38, 180A
6649 MOSs/AOCs.

6650 **ARMY LINGUISTS NOT DOD TRAINED**

6651 B-18. The Army also includes numerous Soldiers of all grades who are proficient in a foreign language and
6652 are receiving a Foreign Language Proficiency Bonus (FLPB) in accordance with AR 11-6 but whose
6653 primary duties do not require foreign language proficiency. They may have attended a civilian school to
6654 learn a foreign language, or they may have acquired proficiency through their heritage. They have the
6655 advantage of being trained Soldiers and are therefore readily deployable throughout the AO.

6656 B-19. These Soldiers may have the specific vocabulary and military skill knowledge for certain linguist
6657 support missions. For example, a supply sergeant who speaks the local language would be an invaluable
6658 asset to the G-4. There are disadvantages in that they already have another job and units are reluctant to
6659 give up personnel especially if they are in key positions. Their capabilities are difficult to assess. Since they
6660 are not required to take the Defense Language Proficiency Test (DLPT) if they are not receiving FLPB, it
6661 is often difficult for the G-1/S-1 to identify them as a linguist or for a non-linguist to judge the level of
6662 their foreign language capability.

6663 **OTHER SERVICE LINGUISTS**

6664 B-20. Other service linguists have the advantage of deployability, loyalty, and in most cases a security
6665 clearance, but must often learn the Army system and specific Army vocabulary. They are also difficult to
6666 obtain since their parent service probably also lacks a sufficient number of trained linguists. Other service
6667 linguists, however, will be valuable in joint operation centers and joint activities. When serving a JTF
6668 headquarters, Army commanders and staffs must be aware of the linguists in the other services in order to
6669 plan for the participation and optimize their employment.

6670 **US CONTRACT LINGUISTS**

6671 B-21. US civilians can be contracted to provide linguist support. They have an advantage over LN hires in
6672 that their loyalty to the US is more readily evaluated, and it is easier for them to be granted the necessary

FOR OFFICIAL USE ONLY

6673 security clearance. However, there are usually severe limitations on the deployment and use of civilians. A
6674 careful assessment of their language ability is important because, in many cases, they use “old fashioned”
6675 terms or interject US idioms. If the linguists are recent émigrés, the use of the language in their country of
6676 origin could be dangerous to them, or their loyalty may reside with their own country, religious group,
6677 tribal affiliations or other close connections when at odds with US interests.

6678 **MULTINATIONAL LINGUISTS**

6679 B-22. Multinational linguists have their own set of advantages and disadvantages. These linguists may be
6680 unfamiliar with the US military system unless they have previously participated in a multinational
6681 operation with US forces. They may have a security clearance, but clearances are not necessarily equal or
6682 reciprocal, automatically guaranteeing access to classified or sensitive information between nations. They
6683 support the command’s interest but may have differing priorities or responsibilities within their assigned
6684 AOs. These linguists also are already fulfilling specific duties for their own nation, which may also have a
6685 shortage of linguists. The major disadvantage to acquiring and maintaining multinational linguist support is
6686 that they are outside the military authority of US forces and not under US military contract. These linguists
6687 will be valuable in multinational operations centers and activities.

6688 **LOCAL NATIONAL CONTRACT LINGUISTS**

6689 B-23. LN hires will provide the bulk of linguist support. They are usually less expensive to hire than US
6690 civilians and will know the local dialect, idioms, and culture. The expertise of these linguists in particular
6691 areas or subject matters can be an asset. However, there are several potential problems with using LN hires,
6692 to include limited English skills and loyalty considerations. Therefore, a screening interview or test is
6693 necessary to determine their proficiency in English. These individuals also must be carefully selected and
6694 screened by CI personnel (with US linguist support) initially and periodically throughout their
6695 employment. Their loyalty is always questionable. Local prejudices may influence them, and they may
6696 place their own interests above those of the US.

6697 **EVALUATING LINGUIST PROFICIENCY**

6698 B-24. Commanders and staffs must understand the Army linguist proficiency evaluation system in order to
6699 effectively plan for and employ linguists. Evaluation and reevaluation of linguist proficiency is covered in
6700 detail in AR 11-6, chapter 5. Language testing is required for all Army personnel in a language-dependent
6701 MOS/AOC, who have received foreign language training at government expense, who are receiving FLPB,
6702 or who are in a language-required position regardless of MOS/AOC. Other Army personnel who have
6703 knowledge of a foreign language are encouraged to take the proficiency test and may work as linguists.

6704 B-25. The Army uses the DLPT to determine foreign language proficiency levels. DLPTs are listed by
6705 foreign language in DA Pam 611-16. In foreign languages where no printed or recorded test exists, oral
6706 proficiency interview tests are arranged. The DLPT is an indication of foreign language capability, but it is
6707 not the definitive evaluation of an individual’s ability to perform linguist support.

6708 B-26. The Army subscribes to the Interagency Language Roundtable’s descriptions of the proficiency
6709 levels for the skills of speaking, listening, reading, and writing a foreign language, which are available at
6710 www.govtilr.org. The plus-level designators, shown as a “+” symbol, are used to designate when a linguist
6711 is above a base level, but not yet to the capability of the next level. For example, 2+ would indicate a better
6712 than limited working proficiency in the foreign language. The six “base levels” of proficiency, as
6713 established by DLPT and/or oral exam, are—

- 6714 ● **Level 0 (No proficiency).** The Soldier has no functional foreign language ability. Level 0+. The
6715 minimum standard for Special Forces personnel indicates a memorized proficiency only.
- 6716 ● **Level 1 (Elementary proficiency).** The Soldier has limited control of the foreign language skill
6717 area to meet limited practical needs and elementary foreign language requirements.

FOR OFFICIAL USE ONLY

- 6718 ● **Level 2 (Limited working proficiency).** The linguist is sufficiently skilled to be able to satisfy
6719 routine foreign language demands and limited work requirements.
- 6720 ● **Level 3 (General professional proficiency).** The linguist is capable of performing most
6721 general, technical, formal, and informal foreign language tasks on a practical, social, and
6722 professional level.
- 6723 ● **Level 4 (Advanced professional proficiency).** The linguist is capable of performing advanced
6724 professional foreign language tasks fluently and accurately on all levels.
- 6725 ● **Level 5 (Functionally native proficiency).** The linguist is functionally equivalent to an
6726 articulate and well-educated native in all foreign language skills; and reflects the cultural
6727 standards of the country where the foreign language is natively spoken.

6728 B-27. The above proficiency base levels designate proficiency in any of the four language skills: listening,
6729 reading, speaking, and writing. The DLPT only evaluates reading and listening skills. These tests currently
6730 do not evaluate linguists above the 3 proficiency level. Oral proficiency interviews evaluate speaking
6731 proficiency and also may be used to provide a listening score. These interviews may provide an evaluation
6732 all the way up to the 5 proficiency level. Most Army linguist DLPT scores show only two skill levels:
6733 listening and reading (for example, 2+/3, or 3/1+). The current Army standard to be considered a qualified
6734 linguist is a level 2.

6735 **ARMY LANGUAGE PROGRAM CHALLENGES**

- 6736 B-28. Implementation of the Army language program results in several major challenges:
- 6737 ● Acquiring sufficient numbers of linguists in the appropriate languages.
 - 6738 ● Anticipating future Army missions and deployments.
 - 6739 ● Accurately forecasting the nature and extent of the Army's future linguist needs.
 - 6740 ● Defining the special aptitude needed to learn foreign languages.
 - 6741 ● The amount of training time required to produce a qualified linguist.
 - 6742 ● The high perishability of foreign language skills.
 - 6743 ● The constant maintenance required to maintain language skills.
 - 6744 ● Linguist retention; foreign languages are a very marketable skill in the civilian sector.
 - 6745 ● Army leadership understanding of Linguist issues.

6746 **LINGUIST SUPPORT FOR INTELLIGENCE AND INFORMATION** 6747 **COLLECTION**

6748 B-29. **Signal Intelligence-Cryptologic Communications Interceptor/Locator 35P:** A cryptologic
6749 communications interceptor/locator analyzes and reports information obtained through intercept of foreign
6750 language communications. Communications intelligence (COMINT) and monitoring for CI purposes,
6751 together with intelligence research and analysis missions, demand highly skilled listening and reading
6752 language capability.

6753 **B-30. Linguist:**

- 6754 ● **Interpreter 09L.** Interpretation is the transfer of meaning from one spoken language into
6755 another spoken language. Units may require interpretation capabilities to support commanders in
6756 communicating with multinational and threat forces. CA and PSYOP units, law enforcement,
6757 medical, logistic, transportation, training, legal, LNOs, and engineer units may also require
6758 interpreter support. Most Services do not currently have an interpreter specialty.
- 6759 ● **Translator 09L.** Translation is the rendering by writing of meaning from one written language
6760 into another language. Units may require translation of documents to support commanders in
6761 communicating with multinational and threat forces. CA and PSYOP units, law enforcement,
6762 medical, logistic, transportation, training, legal, LNOs, and engineer units may also require
6763 translator support. Most Services do not currently have a pure translator specialty.

FOR OFFICIAL USE ONLY

6764
6765
6766
6767

B-31. Human Intelligence: HUMINT collectors specifically include enlisted personnel in MOS 97E, WOs in MOS 35M, WOs in MOS 351M and MOS 351Y, commissioned officers in MOS 35E and MOS 35F, select other specially trained MOSSs, and their Federal civilian employee and civilian contractor counterparts.

6768
6769

Note. These specially trained and certified individuals are the **only** personnel authorized to conduct HUMINT collection operations.

6770

B-32. HUMINT collection operations that require foreign language capability include the following:

6771
6772
6773
6774
6775
6776
6777
6778
6779
6780
6781
6782
6783
6784
6785
6786
6787
6788
6789
6790
6791

- **Interrogation.** Foreign language requirements for interrogation operations include the ability to read foreign language documents for planning and preparation, and support to DOMEX; and listening and speaking abilities for conduct of the interrogation itself. Even if the interrogation is going to be accomplished using an interpreter, it is beneficial for the interrogator to have proficiency in the target language for more complete understanding, and quality control of the interpreter.
- **Debriefing.** Debriefers require foreign language reading, listening, and speaking capability in order to prepare for an carry out debriefings,
- **Liaison.** HUMINT collectors rely heavily on language ability to conduct effective liaison with host country and some officials.
- **MSO.** All foreign language capabilities are required for effective conduct of MSO.
- **Tactical questioning.** Tactical questioning is expedient initial questioning for information of immediate tactical value. HUMINT collectors involved in tactical questioning require foreign language speaking and listening capabilities.
- **Support to DOMEX.** HUMINT collectors require a foreign language reading ability because may CEDs are associated with detainees and other human sources, and a HUMINT collector is often the first person to screen them. HUMINT collectors will screen the documents associated with human sources and will extract information of use to them in their immediate collection operation.
- **Screening.** HUMINT collectors conducting screening must have a foreign language capability in reading, speaking, and listening.

6792
6793
6794
6795
6796

B-33. Counterintelligence: A CI agent is a Soldier in MOS 35L, a WO in MOS 351L, or a commissioned officer in MOS 35E. A CI agent obtains information by direct questioning of a person or persons that may or may not be under the agents' control. Language requirements for CI roles require skill comparable to those being performed by HUMINT specialists. A skilled interpreter can often assist a debriefer. The debriefer skill set is often treated as an ASI, added to either the interrogator or CI specialties.

6797

SUSTAINING MILITARY LINGUIST PROFICIENCY

6798
6799
6800
6801
6802
6803

B-34. Language proficiency is a very perishable skill and diminishes rapidly with lack of use and absence of exposure to the foreign language. In fact, language is quite similar to physical training in that it should be done regularly, if not daily, to maintain capability. Soldiers become a more valuable military asset as they increase their foreign language proficiency. To maintain combat readiness, commanders need to ensure Soldiers have the training time and tools to improve their foreign language skills—as they do for physical training, warrior task training, and other Soldier skills.

6804
6805
6806
6807
6808

B-35. Language labs, on-line foreign newspapers, and foreign radio broadcasts are all examples of language training resources that may be used for this regular training. Additionally, commanders should require all military linguists participate in periodic significant language training events. In-country language immersion training, in-garrison contracted language instructors, and intermediate and advanced language courses taught at the Defense Language Institute Foreign Language Center are some of the

FOR OFFICIAL USE ONLY

6809 options which can be used to meet this training mandate. Funding for language training is available
6810 through language training program funds.

6811 *Note.* Linguists are a critical resource within the military. Linguists will be employed in MOS-
6812 assigned positions or critical linguistic mission tasks and missions and will not be assigned to or
6813 employed in duties as drivers, radio operators, or clerks.

6814 B-36. Developments in technology and the Internet now allow Soldiers to use their foreign language as
6815 often as they can find time. The following are resources that commanders may use to support their
6816 Soldiers' foreign language capabilities:

- 6817 ● In-Country Immersion (Commercial). Several commercial companies provide the opportunity to
6818 send Soldiers to countries where the Soldier may attend language courses and live among the
6819 local residents. For example:
 - 6820 ■ International Center at the University of Utah (www.international.utah.edu).
 - 6821 ■ Worldwide Language Resources (www.wwlr.com).
 - 6822 ■ National Registration for Language Abroad (NRCSA) (www.nrca.com).
- 6823 ● International Standards Organization (ISO)-Immersion. There are commercial and federal
6824 programs that provide foreign country environment within CONUS. For example:
 - 6825 ■ Language Enrichment Activities Program, the Foreign Language Training Center, Fort
6826 Lewis, WA.
 - 6827 ■ Global Language Systems, Bountiful, UT (www.glsnet.globtra.com/).
- 6828 ● Joint Language Centers. Each of the regional operation centers of the NSA has a language
6829 support organization that provides formal language training opportunities. For example:
 - 6830 ■ Fort Gordon, GA (NSA-G).
 - 6831 ■ Schofield Barracks, HI (NSA-H).
 - 6832 ■ Medina, Lackland Air Force Base, TX (NSA-T).
- 6833 ● Local College or University Language Courses. Check with local universities and colleges for
6834 language courses. Some institutions provide the opportunity for custom designed courses for
6835 specific language needs.
- 6836 ● Military Language Refresher Programs. All the four military branches conduct language
6837 enhancement and language refreshes courses at several locations through the Command
6838 Language Program. Many of these programs are conducted in foreign countries as part of the
6839 military in-country immersion program.
- 6840 ● Television Programs. Some of the best and more fun ways of learning a foreign language are
6841 through movies and television programs. Both foreign and US programs (with foreign subtitle or
6842 foreign dubbed) provide the linguist with enjoyable learning environments.
- 6843 ● Computer and Software Language Programs. There are many commercial software programs
6844 currently on the market. Rosetta Stone is available to the military through Army Knowledge
6845 Online (AKO). For example:
 - 6846 ■ Transparent Language (<http://www.transparent.com/>).
 - 6847 ■ Rosetta Stone (www.rosettastone.com).
 - 6848 ■ Tell Me More (www.tellmemorestore.com).
- 6849 ● National Security Agency.
- 6850 ● Military Cryptologic Continuing Education Program (MCCEP). The MCCEP was established to
6851 provide a structure for the professional development of Cryptologic military language analysts.
6852 MCCEP provides career guidance to assist language analysts in broadening and deepening their
6853 target knowledge and job abilities. For example:
 - 6854 ■ <https://www.mccep.org>.

FOR OFFICIAL USE ONLY

-
- 6855
- 6856
- 6857
- 6858
- 6859
- 6860
- 6861
- 6862
- 6863
- 6864
- 6865
- 6866
- 6867
- 6868
- 6869
- 6870
- 6871
- 6872
- 6873
- 6874
- 6875
- 6876
- 6877
- 6878
- 6879
- 6880
- 6881
- 6882
- 6883
- 6884
- SCOLA. A non-profit educational organization that receives and retransmits television programming from around the world in many languages. These programs are available via Internet to students of language study, ethnic communities, and anyone seeking a global perspective. SCOLA's website is www.SCOLA.org; www.podcastdirectory.com.
 - Mobile Training Teams. Contact Defense Language Institute for more information on its mobile training team language courses (<http://www.dliflc.edu>).
 - On-the-Job Training. One of the best, if not the best, methods to help Soldiers increase their language capabilities is through on-the-job training. There are many Federal programs that need linguists. The Reach Language Support Program provides meaningful and challenging translation opportunities to member of the military while providing translation of foreign documents. (rlsp.inbox@us.army.mil). Deployments also provide language proficiency training opportunities.
 - Unit Command Language Program. Almost all Army MI battalions have a Command Language Program Manager (CLPM) who supports military linguists in a personal language program development. The CLPM is the best first step in any Army linguist's career.
 - Joint Language University. The Joint Language University is a cooperative effort between agencies of the Federal Government, DOD, and Academic institutions (<http://jlu.wbtrain.com/>).
 - Internet. There are several language resources available on the internet. For example:
 - Podcasts (www.itunes.com, <http://www.word2word.com/podad.html>).
 - Google. A wealth of language opportunities: music, podcasts, videos, programs, and all sorts of great new technology to support foreign language development (www.google.com).
 - Lingnet. An on-line information service, accessible through the Internet or through direct connection, devoted to meeting the needs of the linguist community (<http://www.lingnet.org>).
 - Langnet. A language learning support system with interactive materials designed for those who want to practice and maintain their target language reading and listening skills (www.langnet.org).
 - Foreign Language Portal. Lists, by foreign language, on the For Official Use Only Army server of foreign language materials (<https://www.us.army.mil/suite/doc/5987514>).

6885 LANGUAGE TECHNOLOGY

6886 B-37. DOD and the Army have limited human foreign language translation capability to meet
6887 requirements. The Sequoyah Foreign Language Translation System mitigates linguistic shortfalls by
6888 expanding the number of language translation points of presence to meet the speech and text translation
6889 requirements for current and future operations. Sequoyah is a suite of existing and developing language
6890 software modules that are integrated, scaleable, tailorable, interoperable, user-friendly, easily deployable,
6891 and available at all echelons. Sequoyah meets the foreign language translation requirements when human
6892 linguists are unavailable. It includes web-enabled, mobile, and portable configurations.

6893 TERMS

6894 B-38. *Machine language translation* is the use of an electronic device to communicate between English
6895 and one or more foreign languages.

6896 B-39. A *Machine Foreign Language Translation System* is a system used to communicate between
6897 English and one or more foreign languages.

6898 B-40. A *one-way device* is a device that contains pre-recorded phrases in a desired target language. Phrases
6899 are selected that best support a situation and are then played as a recording for the target audience.
6900 Methods for selecting and playing a phrase can be touch (using a stylus or buttons) or speech recognition

FOR OFFICIAL USE ONLY

6901 of a user reciting an English phrase. It is important to note that speech recognition in a one-way device will
6902 search for pre-recorded phrases versus actual spontaneous speech translation.

6903 B-41. A *one-way “plus”* or *“1.5 way”* device is a machine foreign language translation system that
6904 utilizes commonly used pre-recorded phrases combined with speech.

6905 B-42. A *two-way device* is a machine foreign language translation system that translates a user’s free
6906 speech into a desired target language and allows the targeted language to be translated back into English
6907 from the intended recipient. This type of device replicates a two-way spoken conversation at the basic
6908 level.

6909 **CAPABILITIES**

6910 B-43. Machine language translation capabilities include simple pre-recorded speech phrase translations
6911 (phrase-based), full two-way free speech translations (free form), and text translations. Various systems
6912 have different capabilities which the user should fully understand before utilizing the devices.

6913 B-44. There are four modes of machine language translation: speech to speech, speech to text, text to text,
6914 and text to speech. Devices may operate in one mode exclusively or in a combination of modes. Speech to
6915 text and text to text devices can be used to monitor foreign broadcast media.

6916 B-45. One-way devices can be loaded with a series of relevant questions and/or commands or instructions
6917 based on the situation. This will ensure that the same questions or commands or instructions are being used
6918 each time. These devices can be used for checkpoint operations, for example, during which a specific
6919 sequence of events occurs repetitively for each person or vehicle passing through the checkpoint.

6920 B-46. Some machine language translation devices can record long portions of speech for later translation
6921 by an interpreter. For example, anti-coalition mosques in Iraq have disseminated tactical information and
6922 anti-coalition messages during operations in the call to prayer. A recording of the call to prayer can later be
6923 analyzed for its content.

6924 **LIMITATIONS**

6925 B-47. All translation devices are limited to the content of their programs. One-way devices depend on the
6926 intended recipient acknowledging the pre-programmed phrases with simple yes or no responses or an
6927 indication that the recipient understands by their actions.

6928 B-48. Sophisticated two-way devices interpret cultural and linguistic nuances as well as simple word for
6929 word translation. Regardless of the accuracy of the device, machines can still only translate words. They
6930 cannot include the unspoken social and cultural subtexts that are also a component of any conversation.
6931 Additionally, local dialects may dictate the meanings of specific words or phrases which may not be taken
6932 into account by the device. Users must always be aware of the possibility of misunderstandings due to
6933 improperly translated words, phrases, or concepts.

6934
6935
6936
6937

FOR OFFICIAL USE ONLY

Glossary

SECTION I – ACRONYMS AND ABBREVIATIONS

2X	Human Intelligence Operations Officer
ABCS	Army Battle Command System
ACC	Army component command
ACE	analysis and control element
ACICA	Army Counterintelligence Coordinating Authority
ADCON	administrative control
AFIST	adversarial, foreign intelligence services, and terrorists
AFMIC	Armed forces Medical Intelligence Center
AKO	Army Knowledge Online
AMC	US Army Materiel Command
AO	area of operation
AOC	area of concentration
AOI	area of interest
ARISC	Army Reserve Intelligence Support Center
ARFOR	Army Forces
ASCC	Army Service Component Command
ASCOPE	areas, structures, capabilities, organizations, people, and events
ASI	additional skill identifier
ASPO	Army Space Program Office
ATCAE	Army Technical Control and Analysis Element
ATCICA	Army Theater Counterintelligence Coordinating Authority
BCT	brigade combat team
BDA	battle damage assessment
BFSB	battlefield surveillance brigade
C&E	collection and exploitation
C2	command and control
CA	Civil Affairs
CBRN	chemical, biological, radiological, and nuclear
CBRNE	chemical, biological, radiological, nuclear, and high-yield explosives
CCDR	combatant commander
CCIR	commander's critical information requirement
CEE	captured enemy equipment
CEM	captured enemy materiel
CFSO	counterintelligence force protection source operations
CI	counterintelligence
CIA	Central Intelligence Agency

CICA	counterintelligence coordinating authority
CJCMEC	Coalition Joint Captured Material Exploitation Center
CJCS	Chairman of the Joint Chiefs of Staff
CMO	civil-military operations
CNO	computer network operations
CNN	Cable News Network
COA	course of action
COG	center of gravity
COMINT	communications intelligence
COMSEC	communications security
CONOP	contingency operation
CONUS	continental United States
COP	common operational picture
DA	Department of the Army
DCGS-A	Distributed Common Ground System-Army
DCS	Deputy Chief of Staff
DEA	Drug Enforcement Administration
DH	Defense HUMINT
DHS	Department of Homeland Security
DIA	Defense Intelligence Agency
DIO	Defence Intelligence Organization, Australia
DIS	Defence Intelligence Staff, United Kingdom
DJIIOC	Defense Joint Intelligence Operations Center
DLPT	Defense Language Proficiency Test
DNI	Director of National Intelligence
DOD	Department of Defense
DOE	Department of Energy
DOMEX	document and media exploitation
DOS	Department of State
DOT	Department of Transportation
DS	direct support
DSO	defense source operation
DVD	digital video disk
EA	electronic attack
ELINT	electronic intelligence
ES	electronic support
EW	electronic warfare
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FFIR	friendly force information requirement
FISINT	foreign instrumentation signals intelligence

FLPB	foreign language proficiency bonus
FMA	foreign materiel acquisition
FME	foreign materiel exploitation
FMP	Foreign Materiel Program
FMT	foreign materiel training
FP	force protection
G-2	Corps or Division Intelligence Officer
GEOINT	geospatial intelligence
GMI	general military intelligence
GS	general support
GSR	General support-reinforcing
HCT	human intelligence collection team
HN	host nation
HOC	human intelligence operations cell
HPT	high-payoff target
HQ	headquarters
HQDA	Headquarters, Department of the Army
HUMINT	human intelligence
HVI	high-value individual
HVT	high-value target
I&W	indications and warnings
ILRT	Interagency Language Round Table
IMINT	imagery intelligence
INR	Bureau of Intelligence and Research (State Department)
INS	Immigration and Naturalization Service
INSCOM	US Army Intelligence and Security Command
IPB	intelligence preparation of the battlefield
ISE	intelligence support element
ISR	intelligence, surveillance, and reconnaissance
J-2	Joint Intelligence Officer
JCMEC	Joint Captured Materiel Exploitation Center
JFC	joint force commander
JIDC	Joint Interrogation Debriefing Center
JHIM	joint, interagency, intergovernmental, and multinational
JIOC	Joint Intelligence Operations Center
JISE	Joint Intelligence Support Center
JRIC	Joint Intelligence Reserve Center
JTF	joint task force
LEA	law enforcement agency
LEP	locally employed personnel
LNO	liaison officer

LTIOV	latest time information is of value
MASINT	measurement and signature intelligence
MCCEP	Military Cryptologic Continuing Education Program
MCIA	Marine Corps Intelligence Agency
MCOO	modified combined obstacle overlay
MDMP	military decision-making process
METT-TC	mission, enemy, terrain and weather, troops and support available, time available, and civil considerations
MI	military intelligence
MIB	military intelligence brigade
MOS	military occupational specialty
MP	military police
MSC	major subordinate command
MSIC	Missile and Space Intelligence Center
MTI	moving target indicator
NAI	named area of interest
NAIC	National Air Intelligence Center
NATO	North Atlantic Treaty Organization
NCO	noncommissioned officer
NCPC	National Counterproliferation Center
NCTC	National Counterterrorism Center
NGA	National Geospatial-Intelligence Agency
NDHQ	National Defence Headquarters, Canada
NGIC	National Ground Intelligence Center
NGO	nongovernmental organization
NIC	National Intelligence Council
NIST	National Intelligence Support Team
NMIC	National Military Intelligence Agency
NRO	National Reconnaissance Office
NRT	near-real time
NSA	National Security Agency
NSG	National System for Geospatial-Intelligence
NST	National Support Team
OCONUS	outside continental United States
OFCO	offensive counterintelligence operations
OMT	operational management team
ONI	Office of Naval Intelligence
OPCON	operational control
OPLAN	operations plan
OPORD	operations order
OPSEC	operations security

OSC	operations support cell
OSINT	open-source intelligence
PA	Public Affairs
PAO	Public Affairs Office
PD/DNI	Principal Deputy/Director of National Intelligence
PIO	police intelligence operations
PIR	priority intelligence requirement
PMESII	political, military, economic, social, information, infrastructure
PMESII-PT	political, military, economic, social, information, infrastructure, with the addition of physical environment and time
POC	point of contact
PSYOP	psychological operation
R&D	research and development
RDEC	research, development, and engineering center
REMBASS	Remotely Monitored Battlefield Sensor System
RF	radio frequency
RFI	request for information
ROE	rules of engagement
RSOC	Regional Security Operations Center
RSP	render-safe procedure
RSTA	reconnaissance, surveillance, and target acquisition
RTCAE	regional technical control and analysis element
S-2	Intelligence Officer
S&TI	scientific and technical intelligence
SAEDA	Subversion and Espionage Directed Against the Army
SALUTE	size, activity, location, unit, time, equipment
SAP	special access program
SAR	synthetic aperture radar
SBCT	Stryker Brigade Combat Team
SCI	sensitive compartmented information
SCID	Strategic Counterintelligence Detachment
SCIF	sensitive compartmented information facility
SECDEF	Secretary of Defense
SIGINT	signals intelligence
SIR	specific information requirement
SOFA	Status of Forces Agreement
SOP	standing operating procedure
SQI	special qualification identifier
SSE	sensitive-site exploitation
TACON	tactical control
TCAE	technical control and analysis element

TECHINT	technical intelligence
TENCAP	Tactical Exploitation of National Capabilities Program
TFCICA	Task Force Counterintelligence Coordinating Authority
THREATCON	threat condition
TOE	table of organization and equipment
TPFDD	time-phased force and deployment data
TSCM	technical surveillance countermeasures
TTP	tactics, techniques, and procedures
URL	uniform resource locator
USACAC	United States Army Combined Arms Center
USAES	United States Engineer School
USAF	United States Air Force
USCENTCOM JIC	United States Central Command Joint Intelligence Center
USCG	United States Coast Guard
USD(I)	Under Secretary of Defense (Intelligence)
USEUCOM JAC	United States European Command Joint Analysis Center
USMC	United States Marine Corps
USJFCOM AIC	United States Joint Forces Command Air Intelligence Center
USNORTHCOM JIC	United States Northern Command Joint Intelligence Center
USPACOM JIC	United States Pacific Command Joint Intelligence Center
USSOCOM JIC	United States Special Operations Command Joint Intelligence Center
USSOUTHCOM JIC	United States Southern Command Joint Intelligence Center
USSPACECOM CIC	United States Space Command Combat Information Center
USSTRATCOM	United States Strategic Command
USTRANSCOM JIC	United States Transportation Command Joint Intelligence Center
V	version
WARNO	warning order
www	world wide web

SECTION II – TERMS

6940

This section to be completed during Final Approved Draft phase.

6941

6942

6943 **term**

definition.

6944

6945 **term**

definition.

6946

6947

References

6949 SOURCES USED

6950 These are the sources quoted or paraphrased in this publication.

6951 ARMY PUBLICATIONS

- 6952 AR 11-6, *Army Foreign language Program*, 14 December 2007
- 6953 AR 27-60, *Intellectual Property*, 1 June 1993
- 6954 AR 380-5, *Department of the Army Information Security Program*, 29 September 2000
- 6955 AR 380-13, *Acquisition and Storage of Information Concerning Non-Affiliated Persons and*
- 6956 *Organizations*,
- 6957 13 September 1974
- 6958 AR 381-10, *U.S. Army Intelligence Activities*, 3 May 2007
- 6959 AR 381-20, *(U) US Army Counterintelligence Activities (S)*, 15 November 1993
- 6960 AR 381-172, *Counterintelligence Force Protection Source Operations and Low-Level Source Operations*,
- 6961 30 December 1994
- 6962 DOD Directive 3115.09, *DOD Intelligence Interrogations, Detainee Debriefings, and Tactical*
- 6963 *Questioning*, 3 November 2005
- 6964 FM 2-22.3, *Human Intelligence Collector Operations*, September 2006
- 6965 FM 2-22.9
- 6966 FM 2-91.6, *Soldier Surveillance and Reconnaissance: Fundamentals of Tactical Information Collection*,
- 6967 10 October 2007
- 6968 FM 3-0, *Operations*, 27 February 2008
- 6969 FM 3-05.102, *Army Special Operations Forces Intelligence*, 31 August 2001
- 6970 FM 3-19.1, *Military Police Operations, Change 1*, 31 January 2002
- 6971 FM 3-90, *Tactics*, 4 July 2001
- 6972 FM 5-0, *Army Planning and Orders Production*, 20 January 2005
- 6973 FM 6-0, *Mission Command: Command and Control of Army Forces*, 11 August 2003
- 6974 FMI 2-01, *Intelligence, Surveillance, and Reconnaissance Synchronization (at CADD)*
- 6975 FMI 2-22.9, *Open-Source Intelligence*, with Change 1 dated 7 May 2008
- 6976 FMI 5-01.1, *The Operations Process*, 16 March 2008
- 6977 TC 2-22.303, *The 2X Handbook*, 31 July 2006
- 6978 DIAM 58-11, *DOD HUMINT Policies and Procedures (S)*
- 6979 DIAM 58-12, *The DOD HUMINT Management System (S)*
- 6980 CJCS Instruction 1301.01, *Policy and Procedures to Assign Individuals to Meet Combatant Command*
- 6981 *Mission-Related Temporary Duty Requirements*, 1 July 2001
- 6982 CJCS Instruction 5120.02A, *Joint Doctrine Development System*, 31 March 2007
- 6983 CJCSM 3500.04C, *Universal Joint Task List (UJTL)*, 1 July 2002
- 6984 NGA Publication 1-0

6985 JOINT PUBLICATIONS

- 6986 JP 2-0, *Joint Intelligence*, 22 June 2007
- 6987 JP 2-03, *Geospatial Intelligence Support to Joint Operations*, 22 March 2007
- 6988 JP 3-0, *Joint Operations, with Change 1*, 13 February 2008

References

- 6989 JP 3-33, *Joint Task Force Headquarters*, 16 February 2007
6990 JP 5-0, *Joint Operation Planning*, 26 December 2006
6991 JP 5-00.2, *Joint Task Force Planning Guidance and Procedures*, 13 January 1999

DOCUMENTS NEEDED

- 6992 These Documents must be available to the intended users of this publication.
6993
6994
6995 DA Form 2028, *Recommended Changes to Publications and Blank Forms*

READINGS RECOMMENDED

- 6996 These sources contain relevant supplemental information.
6997
6998 AR 350-1, *Army Training and Education*, 9 April 2003
6999 AR 380-5, *Department of the Army Information Security Program*, September 2000
7000 AR 380-10, *Technology Transfer, Disclosure of Information, and Contacts with Foreign Representatives*,
7001 15 February 2001
7002 AR 380-15. (C) *Safeguarding NATO Classified Information*, 1 March 1984
7003 AR 380-28, *Department of the Army Special Security System*, 12 December 1991
7004 AR 380-40, *Policy for Controlling and Safeguarding Communications Security (COMSEC) Material*,
7005 22 October 1990
7006 AR 380-49, *Industrial Security*, 15 April 1982
7007 AR 380-53, *Telecommunications Security Monitoring*, 29 April 1998
7008 AR 380-67, *Personnel Security Program*, 9 September 1988
7009 AR 381-1, *Security Controls on Dissemination of Intelligence Information*, 12 February 1990
7010 AR 381-12, *Subversion and Espionage Directed Against the US Army (SAEDA)*, 15 January 1993
7011 AR 381-14, *Technical Counterintelligence (TCI)*, 30 September 2002
7012 AR 381-45, *Investigative Records Repository*, 25 August 1989
7013 AR 381-47, (U) *US Army Offensive Counterespionage Activities (S)*, 30 July 1990
7014 AR 381-100, (U) *Army Human Intelligence Collection Program (S)*, 15 May 1988
7015 AR 381-102, (U) *US Army Cover Support Program (S)*, 10 January 1991
7016 AR 381-143, *Military Intelligence Nonstandard Material Policies and Procedures*, 1 December 1986
7017 AR 614-115, *Military Intelligence Excepted Career Program*, 12 April 2004
7018 AR 614-200, *Military Intelligence Civilian Excepted Career Program*, 30 September 2004
7019 DA Pam 381-15, *Foreign Military Intelligence Collection Activities Program*, 1 June 1988
7020 DA Pam 611-16, *Handbook of Army Personnel Test*, 1 April 1985
7021 Executive Order 12333, *United States Intelligence Activities*, 4 December 1981
7022 DOD Directive 2310.1, *DOD Program for Enemy Prisoners of War (EPOW) and Detainees*
7023 (*Short Title: DOD Enemy POW Detainee Program*), 18 August 1994
7024 DOD Directive 2310.1E, *The Department of Defense Detainee Program*, 5 September 2006
7025 DOD Directive 5100.20, *The National Security Agency and the Central Security Service*,
7026 23 December 1971
7027 DOD Directive 5100.77, *DOD Law of War Program*, 9 December 1998
7028 DOD Directive 5240.1, *DOD Intelligence Activities*, 3 December 1982
7029 DOD Regulation 5240.0-R, *Procedures Governing the Activities of DOD Intelligence Component*
7030 *That Affect United States Persons*, December 1982
7031 FM 27-10, *The Law of Land Warfare*, July 1956
7032 NGA GEOINT Basic Document Publication 1, September 2006
7033 Title 32, *United States Code* (available online)
7034 Further information and links to many of the above publications can be found at:
7035 <http://www.dami.army.pentagon.mil/offices/dami-cd/>

7036

7037

ARTEPS, MTPs and other intelligence training products are available at the Reimer Digital Library

7038

<http://www.adtdl.army.mil>

7039

DOCUMENTS TO BE PUBLISHED

7040

FM 2-01.3, *Intelligence Preparation of the Battlefield*

7041

FM 2-01.301, *Tactics, Techniques, and Procedures of Intelligence Preparation of the Battlefield*

7042

FM 2-22.2, *Counterintelligence*

7043

FM 2-22.4, *Technical Intelligence*

7044

FM 7-15, *The Army Universal Task List*

7045

FM 2-33.4, *Intelligence Analysis*

7046

FMI 2-91.501, *Intelligence Support to Civil Support Operations*

7047

TC 2-22.201, *Counterintelligence Operations and Collection Activities (S//NF)*,

7048

TC 2-22.302, *Controlled Military Source Operations (S//NF)*

7049

TC 2-22.101, *Biometric Enabled Intelligence*

7050

7051

Index

A

actionable intelligence, vi, 1-19, 2-13

analysis of
 area of operations, A-8

areas, structures, capabilities, organizations, people, events
 civil considerations, A-9

Army intelligence enterprise, 1-27

B

biometrics, 1-30

C

characteristics of effective intelligence, vi, 1-18, 1-19

civil considerations, A-9

course of action
 wargaming, A-15

D

database development, 1-10

Distributed Common Ground Station-Army, 1-10, 1-30, 1-31, 4-4, 4-15, 13-5

E

effective intelligence, 2-1, 3-2, 4-3

enemy course of action, A-14, A-15

F

friendly course of action, A-11, A-12, A-15

G

generate knowledge, 1-11, 4-1, 4-2, 10-4, 11-1, 11-2, 12-4, 13-4, 13-5

I

information requirements, 1-14, 4-12, 4-13

intelligence architecture, 1-10, 2-1, 4-7, 4-15
 joint, 2-15
 reports, 4-14
 seamless, 4-14
 tactical, 8-4
 theater, 2-21

intelligence disciplines, vi
 all-source intelligence, 1-28
 counterintelligence, 1-28, 2-1
 geospatial intelligence, vi, vii, 1-28, 2-4, 8-2, 8-3, 8-5
 human intelligence, 1-28, 2-1
 imagery intelligence, vii, 1-28
 measurement and signature intelligence, vii, 1-28, 1-29, 2-1, 10-1
 open-source intelligence, vi, vii, 1-28, 1-29
 signals intelligence, vii, 1-28, 1-30
 technical intelligence, 1-28, 1-30

intelligence operations
 fundamentals of, v

intelligence overwatch, 1-10, 1-13

intelligence process, v, vi, 2-1
 and measurements and signatures intelligence, 10-4
 and operations process, 4-1, 4-2
 and signals intelligence, 12-3
 and technical intelligence, 13-3
 functions, 4-12
 steps, 4-1

intelligence readiness, 1-8, 2-10, 2-17, 2-23
 overview, 2-1

intelligence requirements, vi, 1-14, 2-7, 2-13, 2-19, 4-2, 4-13, 6-6, 6-11

intelligence running estimate, A-8

intelligence survey, vi, 4-2, 13-4

intelligence warfighting
 function, v, vi, 1-1, 1-5, 1-6
 and intelligence tasks, 1-8
 considerations, 4-3
 standards, 1-18
 subtasks, 1-8
 tasks, 1-6

within full spectrum operations, 2-1

M

military aspects of terrain, A-8

mission variables, vi, 1-5, 1-12, 3-2, 10-4

O

operational environment, v, 1-1
 analysis of, 1-1
 components, 1-5
 definition, 1-1

operational variables, 1-1, 1-5

P

perform intelligence, surveillance, and reconnaissance, 1-6, 1-9, 1-14

police intelligence operations, 1-13

priority intelligence requirements, 1-13, 1-14, 2-19

R

requirements, 1-8
 commander's critical information, 1-10, 1-14
 commander's intelligence, 1-8
 force protection, 1-16
 format, 1-10
 intelligence synchronization, 1-14
 operational, 1-19
 priority intelligence, 1-13
 reporting, 1-15
 specific information, 1-14

S

situational awareness, A-9

staff weather officer, A-10

support to force generation, 1-6, 1-8, 1-9

support to situational understanding, 1-6, 1-9, 1-12

support to targeting and information tasks, 1-6, 1-9, 1-17

T

terrain analysis, A-8, A-10

threat
capabilities, A-11
characteristics, A-11, A-13

threat course of action, A-14

analysis, A-10

W

weather

FINAL DRAFT

FINAL DRAFT