



Joint Information Operations Planning Handbook

July 2003

**Joint Command, Control and
Information Warfare School**

Joint Forces Staff College

Joint Information Operations Planning Handbook

Prepared and Maintained by the
Information Warfare Division

of the

Joint Forces Staff College
National Defense University
Norfolk, Virginia

Table of Contents

Table of Contents	i
Preface iii	
Planning Handbook Objectives	iii
Acknowledgements	iii
Changes Since the Last Edition	iii
Providing Feedback.....	iv
Chapter I – Basics of Information Operations.....	I-1
Introduction.....	I-1
Lessons Learned.....	I-3
Objective.....	I-3
Guidance	I-3
Organizations.....	I-3
Timing and Phasing	I-3
Coordination.....	I-3
Resources.....	I-4
Training and Education.....	I-4
Planning.....	I-4
Operations Security	I-4
Psychological Operations	I-4
Military Deception	I-5
Electronic Warfare	I-5
Physical Attack / Destruction.....	I-6
Computer Network Attack (CNA).....	I-6
Civil Affairs (CA).....	I-6
Public Affairs (PA).....	I-6
Counterintelligence (CI).....	I-6
Counter-deception	I-6
Counter-propaganda.....	I-7
Information Assurance (IA)	I-7
Chapter II – Organizing a Staff for Information Operations	II-1
The Information Operations Cell	II-1
Information Operations Cell Chief.....	II-2
IO Cell Responsibilities	II-3
Information Coordination Board	II-4
Information Operations Working Group (IOWG).....	II-4
Targeting Integration	II-5
Methodology	II-5
Lists related to targeting.....	II-6
External Augmentation	II-7
Chapter III – Planning Joint Force Information Operations: Integrating Information Operations in the Staff Planning Process.....	III-1
Information Operations Planning.....	III-1
Intelligence Support.....	III-6
Offensive Information Operations	III-6
Defensive Information Operations.....	III-6
Chapter IV – Integrating Information Operations in JOPES Deliberate/Crisis Action Planning/Execution on a Unified Command Staff	IV-1
Introduction.....	IV-1
Planning Basics.....	IV-9
JOPES Deliberate Planning Process	IV-13

JOPES Crisis Action Planning Process.....	IV-65
Executing the Plan.....	IV-69
Chapter V – Joint Information Operations Attack Planning Process	V-1
Introduction.....	V-1
The Five Steps of the Joint Information Operations Attack Planning Process.....	V-1
Step One: Identify the Offensive Information Operations Objectives.....	V-3
Step Two: Generate the Offensive Information Operations Tasks	V-5
Step Three: Identify the Information Operations Targets.....	V-10
Step Four: Identify the IO Assets, Derive the IO Sub-tasks, and Prepare the Candidate Master IO Target List	V-13
Step Five: Conduct Equity Review	V-18
Class Slides.....	V-18
Chapter VI – Joint Information Operations Defensive Planning Process	VI-1
Introduction.....	VI-1
The Five Steps of the Joint Information Operations Defensive Planning Process	VI-2
Step One: Identify the Defensive Information Operations Objectives.....	VI-3
Step Two: Generate the Defensive Information Operations Tasks.....	VI-6
Step Three: Identify Assets to be Protected and Conduct Risk Assessment	VI-9
Step Four: Select Protection Measures and Derive Defensive Information Operations Sub-tasks as Required.....	VI-11
Step Five: Prepare the Master Protection List and Conduct Equity Review	VI-16
Class Slides.....	VI-17
Chapter VII – Annexes and Appendices.....	A-1
Annex A – Information Operations Estimate Process	A-1
Appendix 1 – Operations Security.....	A-7
Appendix 2 – Psychological Operations.....	A-11
Appendix 3 – Deception.....	A-15
Appendix 4 – Electronic Warfare.....	A-19
Appendix 5 – Physical Destruction.....	A-23
Appendix 6 – Information Assurance	A-25
Appendix 7 – Computer Network Attack	A-27
Appendix 8 – Special Information Operations	A-29
Annex B – Glossary.....	B-1
Abbreviations and Acronyms	B-1
Joint Publication References	B-12
Joint Publication Availability.....	B-13
Match IO Effects Words with IO Capabilities and Related Activities	B-13
IO Effects Definitions	B-14

Preface

Planning Handbook Objectives

This planning Handbook is not doctrine. It is intended to be a collection of best practices, experiences and lessons learned. Previous editions have been used as the basis for real-world planning. This Handbook provides the following:

- **Chapter I – Basics of Information Operations** is a brief overview of the capabilities required to successfully conduct Information Operations within the context of a Joint Force, and a summary of some lessons learned. A new draft section on IO objectives, tasks, measures of effectiveness, and concept of operations has been added.
- **Chapter II – Organizing a Staff for Information Operations** covers the JF/Unified Command IO Cell, Information Coordination Boards or cells and includes a discussion on the integration of IO into the targeting process.
- **Chapter III – Planning Joint Force Information Operations** provides both doctrinal and emerging Tactics, Techniques, and Procedures, a discussion of the Commander's responsibilities and presents some thoughts on processes and priority setting.
- **Chapter IV – Integrating Information Operations in JOPES Deliberate/Crisis Action Planning/Execution on a Unified Command Staff** is a step-by-step guide for Unified Command level IO cells using JOPES.
- **Chapter V – Joint Information Operations Attack Planning Process** is a non-technical guide to planning Offensive IO.
- **Chapter VI – Joint Information Operations Defensive Planning Process** is a non-technical guide to planning Defensive IO.
- **Chapter VII – Annexes and Appendices:**
 - **Annex A – The Information Operations Estimate Process** is a step-by-step guide to developing IO estimates of supportability suited for JF or Unified Command IO Cells.
 - **Annex B – Glossary** of Abbreviations, Acronyms, References, Effects, and useful Definitions.

Since this Handbook is not doctrine, it should not be construed as such.

Acknowledgements

The Information Warfare Division staff of the Joint Command, Control and Information Warfare School at the Joint Forces Staff College would like to thank those members of the U.S. Joint Forces Command staff whose work and ideas have been incorporated into this Handbook.

We would also like to thank the Joint Information Operations Center for providing the materials for Chapter V on the Joint Information Operations Attack Planning Process and Chapter VI on the Joint Information Operations Defensive Planning Process.

Changes Since the Last Edition

July 2003: Continued editorial changes: "C/C" was revised to "CC". Navy commands were renamed as appropriate. SPACECOM references were changed to STRATCOM or NORTHCOM. Updated bulleted IO planning material on pages III-2 and III-3. Revised Annex A (IO Estimate Process) to more closely match the IO planning process. Moved the "IO Objectives, Tasks, MOEs and Concept of Operations" section from Chapter I to the Annex A introduction and revised it.

July 2002: This version consists primarily of typographical corrections and minor clarifications. Additional acronyms were added to the Glossary. References to "CINC" were changed to "Combatant

Command,” “Combatant Commander,” or abbreviated as “C/C.” References to “NCA” were changed to “SECDEF.”

January 2002: This was a complete reissue of the *Joint Information Operations Planning Handbook*. The previous edition was dated March 2001. The format has been changed to allow easier reading and the inclusion of more material.

- ❑ Chapter I has had a draft section added on “IO Objectives, Tasks, MOEs and Concept of Operations”
- ❑ Chapter II has been completely revised and updated
- ❑ Chapter IV has had significant updates to match the JCIWS JIWSOC IO Planning Class and the new Joint IO Planning Course
- ❑ Chapter V on the Joint Information Operations Attack Planning Process is new and includes the slides for the Joint IO Planning Course
- ❑ Chapter VI (formerly Chapter V) has been modified to include slides from the inaugural session of the Joint IO Planning Course
- ❑ Chapter VII, Annex B Glossary has a significantly expanded list of acronyms as well as useful definitions of IO Effects. Two essays previously included as Annexes C and D have been removed until they can be updated.

Providing Feedback

Please provide us comments and feedback for additions, deletions or corrections to this Handbook.

IW Division
JFSC/JCIWS/IW
7800 Hampton Blvd.
Norfolk, VA 23511-1702

DSN: 646-6333
Commercial: 757-443-6333
Email: JCIWS-IW@jfsc.ndu.edu

Chapter I – Basics of Information Operations

Introduction

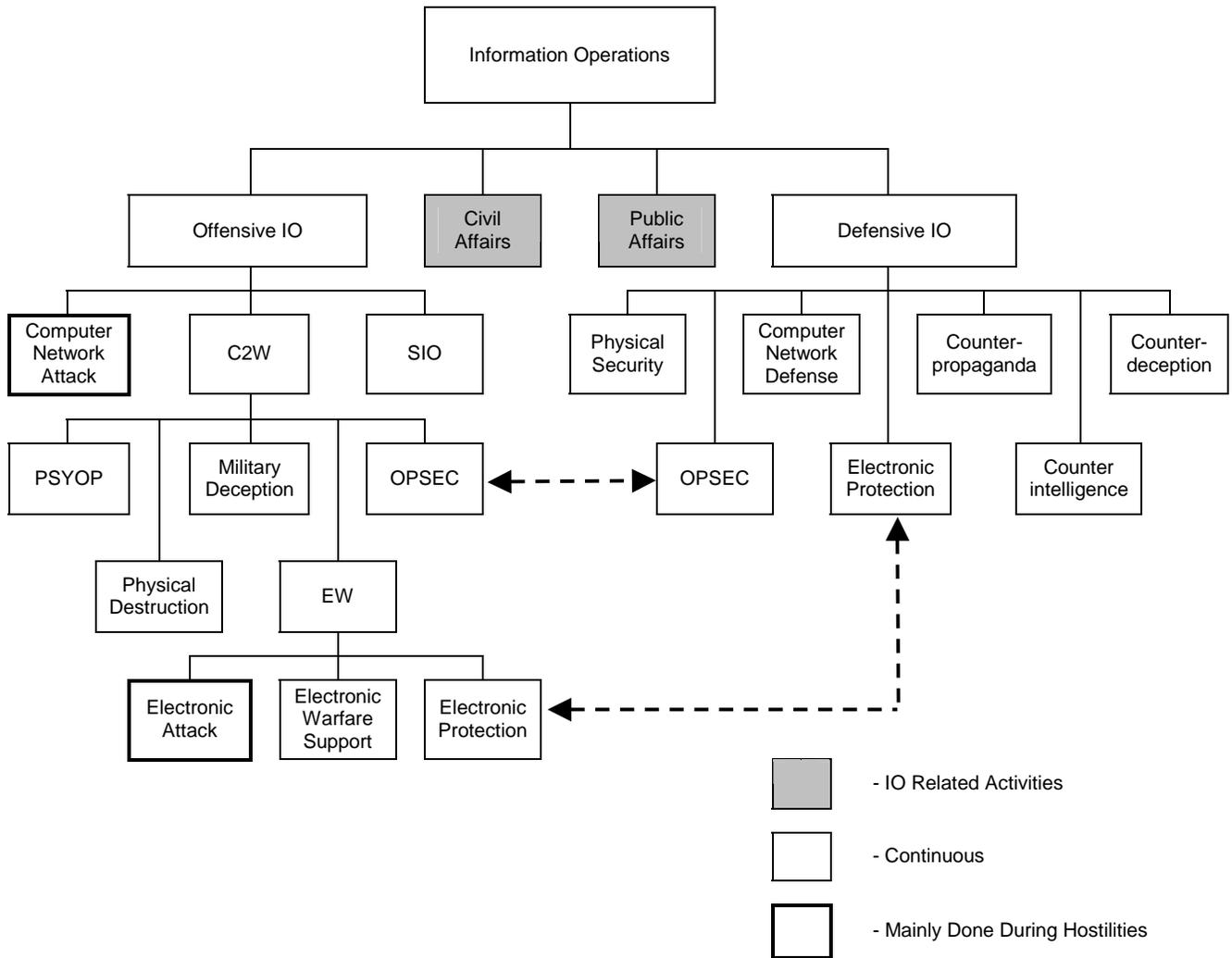
Information Operations (IO) is critical during all phases of an operation across the spectrum of war. IO involves actions taken to affect adversary information and information systems while defending ones own information and information systems. U.S. dependence on information and information systems exposes the U.S. to a wide range of adversaries – hackers, criminals, vandals, terrorists, transnational groups and nation states. Consequently, a coherent IO strategy, integrated with operations, is essential to counter these asymmetrical adversaries.

The Information Operations and Information Warfare capabilities and related activities must be synchronized, coordinated and integrated to effectively support a commander. Additionally, continuous coordination with Intelligence (J2), Communications (J6), the Joint Planning Group, and the IO related activities of Public Affairs and Civil Affairs is essential. Because of the tremendous coordination, synchronization, and deconfliction required to make IO work, we commonly refer to IO as an “integrating strategy” for planning and execution.

When the term Information Operations first came into common use, the emphasis was on emerging technology and the systems that the two or more sides in a conflict or crisis might use against each other. The operational center of gravity followed a Clausewitzian paradigm; that is the destruction of adversary forces in the field, and confusing, blinding and degrading the adversary's command and control structure. Lessons learned from joint exercises and real-world operations concluded that although the hardware aspects of IO are important, the human dimension was not getting the emphasis it deserved. Recent IO operations have included increased emphasis on the adversary decision-making process. Balancing the efforts of both technology (hardware, software and systems) and the human aspects (perception management) is critical to the operation's success.

The future that is conceptualized on the premise that modern and emerging technologies – particularly information specific advances – should make possible a new level of joint operations capability. Underlying a variety of technological innovations is information superiority – the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. U.S. forces must continue to explore innovative ways of applying the full range of IO techniques and procedures in direct support of all operations as they counter increasing and expanding adversaries.

This Handbook provides a quick reference that describes the significant impact Information Operations can have on operations and provide some ideas on how to best use this methodology in the process of planning and executing joint operations.



Note: *The division of the IO Cell into offensive and defensive sub-components is shown for the purpose of highlighting the functions only. We do not advocate splitting the cell into these two disciplinary areas.*

Lessons Learned

Some lessons learned from Information Operations include the following:

Objective

Objective is a principal of war espoused by the great military thinker Carl von Clausewitz. Put simply, the principle of objective means that every action in an operation should ultimately contribute towards the accomplishment of a single aim. The commander's objective(s) answer the "what" a commander wishes to accomplish. The commander's strategy answers the "how" the commander intends to accomplish his objective. Every action planned by the IO Cell must be tied to accomplishing the commander's objective(s). Likewise, the commander's objectives must be tied to national security objectives and the National Security Strategy (NSS) given by the President. This is accomplished through the Strategy-to-Task planning methodology. Along with stating his objectives to the IO Cell and other staff planners, the commander should issue planning guidance.

Guidance

There are no established tactics, techniques and procedures (TTP) for employing IO. The IO Cell must have the guidance from the JF Commander, the Combatant Commander, and the SECDEF in order to function properly. The IO Cell should seek guidance early and continuously as the situation changes to enable it to make the most efficient use of its valuable resources. Coordination within the IO Cell is essential to ensure that all possible factors are given appropriate consideration. (e.g., the Joint Force Air Component Commander (JFACC) might want to "take out" all the C2W nodes, the Joint PSYOP Task Force (JPOTF) Commander might want to exploit some of them, and the Staff Judge Advocate (SJA) says the Rules of Engagement (ROE) don't support "taking out" any of them.)

Organizations

There are numerous organizations both internal and external to a Unified Command or Joint Force (JF) components that will have a direct impact on the success of the IO effort. (See Page II-1 for discussion of the JF IO Cell concept. See Page IV-1 and following, for a discussion of the Unified Command IO concept.) Properly coordinating and utilizing these assets is a monumental task that should not be underestimated. Obviously, one must include all those that are applicable, but care should be taken not to include some just for the sake of inclusion. Ensuring proper representation by each of the applicable organizations is the responsibility of the IO Cell Officer.

Timing and Phasing

Information Operations are most effective when they are begun during the early part of the decision making process. Along with the complexity of the intelligence gathering required, the development and implementation of the Information Operations plan as early as possible is critical. Just as traditional planning includes considerations for specific events, responses and phases, so should IO planning. Each phase of an operation should include a complete review of the IO plan. This should include changes in ROE, commander's intent, and the political, cultural and economic factors.

Coordination

Coordinating IO requirements within the operations plan is essential. The initial coordination should occur within the IO cell and a significant portion of this coordination should be directed towards the Joint Targeting Steering Group (JTSG), Joint Targeting Coordination Board (JTCB) and the Joint Planning Group (JPG). IO planners must be integrated into the JPG, as there is only one plan produced, into which IO is carefully woven. Coordination may be divided into three types: initial organization and planning, plan adjustment during execution, and transition back to peace. Because the focus of IO is on peacetime operations, much of the coordination will take place outside of the Department of Defense

(DoD), in the interagency realm. A commander's Information Operations may require coordination with the Departments of State, Commerce, and Energy, just to name a few. There may also be requirements for coordination with the CIA, FBI, Treasury Department, Justice Department and a host of others. For this reason, the lead agency for IO may frequently be other than the DoD.

Resources

On one hand, one might argue that there are never enough assets to go around. On the other, IO assets can be found at all levels of DoD and across the interagency environment. Remember that resources include hardware, software, personnel, time, and many other examples, depending on the situation. Proper use and protection of these assets is essential. Because some of the effects of IO may extend beyond the CC's AOR, the IO cell should consider collateral effects when planning.

Training and Education

This part is often left out of the overall IO plan. Training personnel on the IO plan and formalizing training will strengthen teamwork. Do not let training and education take a back seat to operational requirements. Without proper training and a solid understanding of IO by the IO team players, IO will fail.

Planning

IO planning must occur simultaneously with and integrated into operations planning. Staffs create single, integrated plans and IO is an essential part of each plan. One of the keys to successful integration of IO into the JOPES process is ensuring that coordination occurs at the interagency, Unified Command, Sub-Unified Command, Functional Command, JF, subordinate JF, and component levels. This vertical coordination is just as critical as the horizontal coordination is at each level. Chapter III describes in detail the tasks required to integrate IO into JOPES at the JF level. Chapter IV discusses integrating IO into JOPES at the Unified Command level.

Operations Security

To prevent adversaries (or potential adversaries) from gaining valuable information about friendly operations, the staff must include OPSEC in mission planning as early as possible and then make revisions as necessary to support changes in current operations and adversaries. The OPSEC process is comprised of five major activities:

- Identification of critical friendly information
- Analysis of adversaries
- Analysis of vulnerabilities
- Assessment of risk
- Application of appropriate OPSEC protective measures and countermeasures

Psychological Operations

PSYOP conveys selected bits of factual information to an adversary in order to manage his/her perceptions and behavior. Goals in a PSYOP campaign should be to:

- Reduce efficiency of opposing forces
- Further the U.S. and/or multinational war effort by modifying or manipulating attitudes and behavior of selected audiences
- Facilitate reorganization and control of occupied or liberated area in conjunction with civil-military operations
- Obtain the cooperation of allies or coalition partners and neutrals in any PSYOP effort
- Support and enhance humanitarian assistance, foreign internal defense and/or foreign nation assistance to military operations

Steps to accomplishing a successful PSYOP operation include:

- Development of a comprehensive PSYOP campaign
- Complete research and analysis of target audiences
- Development of methods to convey or deny information
- Establishing production development requirements
- Establishing dissemination plan
- Coordinating and deconflicting with all other applicable organizations (Public Affairs, Civil Affairs, non-governmental organizations, etc.)

PSYOP and Perception Management – PSYOP is the very essence of perception management and therefore is a key capability in any offensive IO operation. PSYOP must be carefully coordinated and deconflicted with all Public Affairs messages. PSYOP messages and themes must be totally complementary with the messages and themes conveyed by a joint commander's Public Affairs system. This supports the principle of objective and ensures that our adversaries do not receive mixed messages from our perception management efforts that they might interpret incorrectly.

Military Deception

Deception is used to deliberately mislead adversary military decision-makers as to friendly military capabilities, intentions, and operations. Successful deception plans normally include surprise, security, mass and economy of force. Guidance for planning and executing deception operations are based on the following six principles:

- **Focus:** Target the adversary decision-maker – not the intelligence system.
- **Objective:** To cause the adversary to take (or not to take) specific actions.
- **Centralized Control:** Deception must be directed and controlled by a single element.
- **Security:** Successful deception depends on the adversary not knowing he is being deceived. This requires strict security – tied directly to the OPSEC effort.
- **Timeliness:** In deception, timing is everything. Time must be taken into account for the deception to occur, the adversary's intelligence system to collect, analyze, and report, for the adversary decision maker to react, and for the friendly intelligence system to detect the action resulting from the adversary's decision.
- **Integration:** Deception planning must occur simultaneous with operation planning and must be fully integrated. The deception must not be identifiable as the "one that doesn't belong."

In addition, deception operations should be closely coordinated with your PSYOP campaign and Civil Affairs efforts so as not to inadvertently undermine the relationship with the civilian population or with the host-nation military authorities.

Electronic Warfare

Electronic Warfare refers to any military action involving the use of electromagnetic or directed energy to control the electromagnetic spectrum or to attack the adversary. EW includes three major subdivisions:

- **Electronic Attack (EA):** Using the electromagnetic spectrum or directed energy to attack personnel, facilities or equipment with the intent of degrading, neutralizing or destroying adversary capabilities.
- **Electronic Protection (EP):** Actions taken to protect personnel, facilities, and equipment from any effects of friendly or adversary employment of electronic warfare that degrade, neutralize or destroy friendly combat capability.
- **Electronic Support (ES):** Under direct control of an operational commander, actions taken to search for, intercept, identify and locate sources of intentional and unintentional radiated electromagnetic energy for the purpose of adversary recognition.

In peacetime, government organizations, international treaties, and conventions control the use of the electromagnetic spectrum. EW used in support of military operations other than war normally is restricted to actions that do not violate the peacetime use of the spectrum. The only exception to this under peacetime ROE apply when action is necessary to protect the forces. During military operations that involve hostilities, control of the electromagnetic spectrum will often be contested and the full range of EW actions may be available. The type and level of EW actions appropriate to a particular military operation depend on the adversary which adversary forces pose, the reliance of adversary forces on the use of the electromagnetic spectrum, and the objectives of the operation.

Physical Attack / Destruction

In theory, the last resort in the commander's choice of assets, destruction should be considered, just like the "soft kill" IO capabilities as a viable choice for conducting IO. Again, ROE will play a major role in determining if destruction is available during a particular phase of an operation. Destruction must be supported by other capabilities and related activities of IO. At a minimum, IO planners should consider supporting destruction with PSYOP and Public Affairs.

Computer Network Attack (CNA)

Computer Network Attack is difficult to plan, requires extensive lead-time, and requires an incredible amount of intelligence. Nevertheless, it is another IO option available to the commander. Even when all is in place, CNA may be restricted by legal considerations. International law on CNA is not fully developed and some countries may consider CNA as an act of war.

Civil Affairs (CA)

As a related activity of IO, CA is a tool available to help support the commander's IO objectives. CA is used to gain and maintain support for United States' operations in friendly, neutral, and hostile foreign areas. Put in familiar terms, CA helps the U.S. military and the U.S. Government to "win the hearts and minds" of governments and populations. Civil Affairs operations provide economy of force and may help to reduce friction and deter hostile acts that could necessitate employing conventional military forces.

Public Affairs (PA)

PA provides both internal and external audiences the unblemished truth regarding DoD activities and military operations. It is a related activity of IO that may be used to amplify the effects of CA activities and all of the IO capabilities except deception, as it is against DoD policy to use PA to support disinformation. Public Affairs should be coordinated closely with PSYOP to ensure consistency of messages and with a command's OPSEC program to ensure that critical friendly information is not inadvertently revealed. PA can be an effective means to reduce the effect of adversary propaganda.

Counterintelligence (CI)

CI is information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, foreign persons, or international terrorist activities. Counterintelligence is an integral part of IO. CI is a critical part of any commander's education, training and awareness program for IO. CI helps protect critical information and informs friendly personnel as to an adversary's capabilities and methodologies for collecting that information.

Counter-deception

Counter-deception includes those efforts to negate, neutralize, diminish the effects of, or gain advantage from a foreign deception operation. Counter-deception does not include the intelligence function of identifying foreign deception operations.

Counter-propaganda

Counter-propaganda activities identifying adversary propaganda contribute to situational awareness, and serve to expose adversary attempts to influence friendly populations and military forces. Counter-propaganda consists of specific PSYOP and/or Public Affairs activities aimed at countering hostile PSYOP or propaganda directed towards the United States, its allies or coalition partners, their individual and collective military forces, and friendly populations. Counter-propaganda activities must be carefully formulated and closely coordinated between the joint force commander's PSYOP and Public Affairs organizations. In many cases, the correct response to hostile PSYOP or propaganda may be to totally ignore it so as to avoid lending it credibility. In other instances, direct PSYOP and/or Public Affairs messages may be developed to counter an adversary's misinformation. The ultimate decision on how best to respond will rest with the joint force commander based upon recommendations developed through the close coordination of the IO Cell and the supporting PSYOP unit or Joint PSYOP Task Force (JPOTF).

Information Assurance (IA)

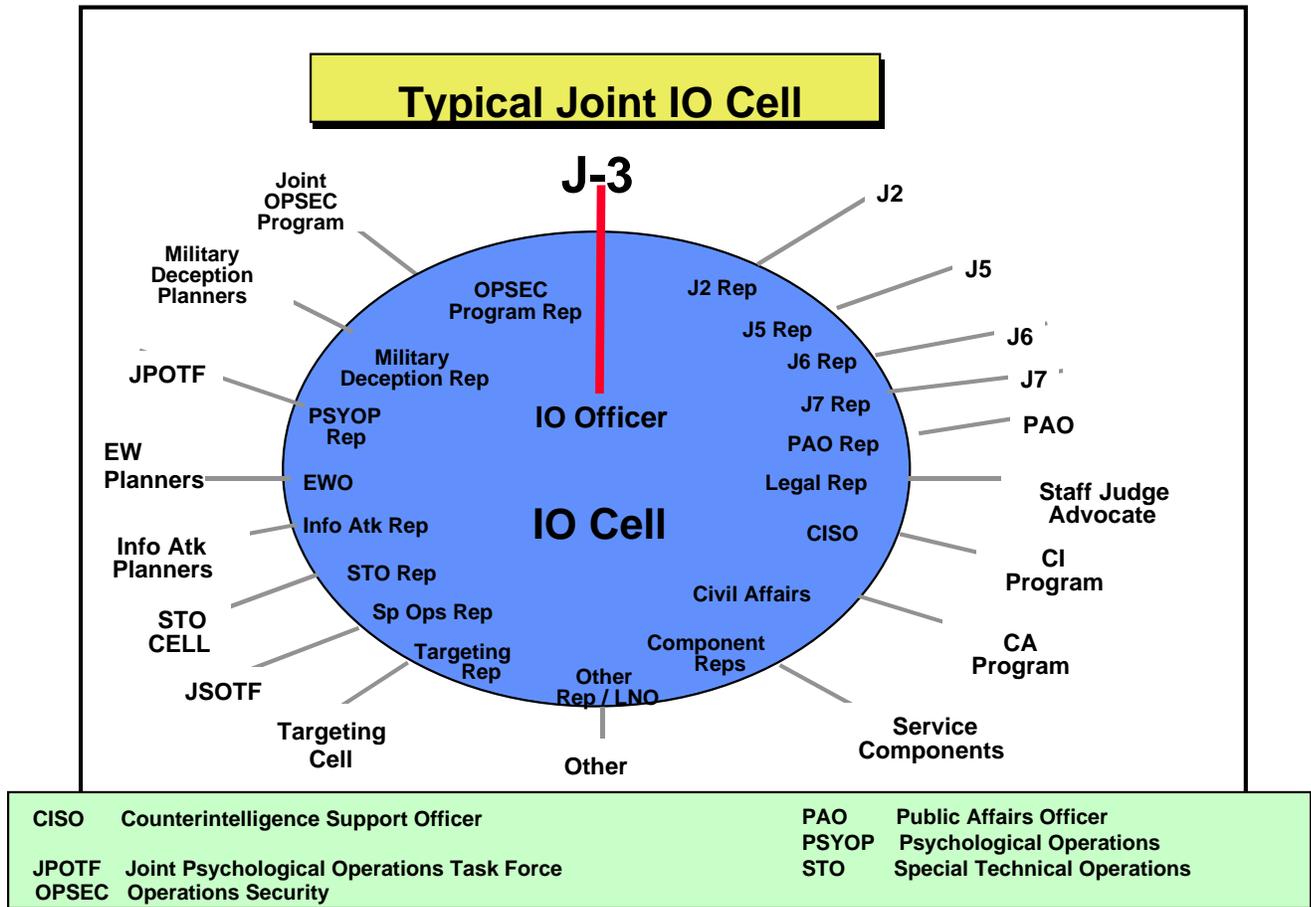
IA protects and defends information and information systems by ensuring their availability, integrity, identification and authentication, confidentiality, and non-repudiation. This includes providing for the restoration of information systems by incorporating protection, detection, and reaction capabilities. IA employs technologies and processes such as multilevel security, access controls, secure network servers, and intrusion detection software. IA responsibility lies mainly within the realm of the J6 Communications Staff Officer and is not discussed in detail in this Handbook.

This page is intentionally blank

Chapter II – Organizing a Staff for Information Operations

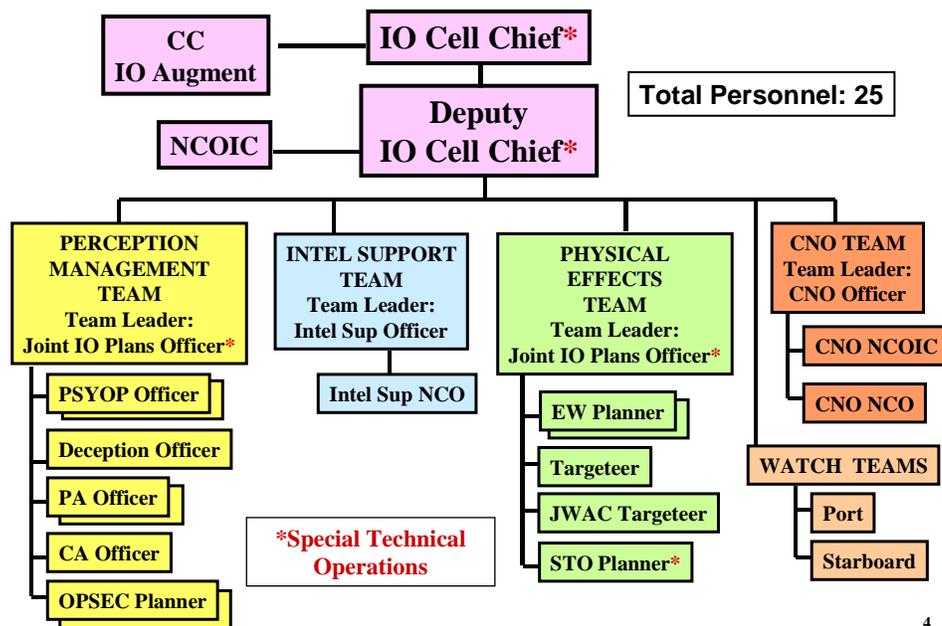
The Information Operations Cell

A fully functional IO Cell integrates a broad range of potential IO actions and activities that contribute to fulfilling the Joint Force Commander's (JFC) objectives, guidance and intent (Purpose, Method, and End State) within a Joint Operations Area (JOA). Ensuring that IO is an integral part of all joint military operations requires extensive planning and coordination among all the elements of the staff. The IO cell is formed from representatives from each staff element, component and supporting agencies responsible for integrating IO capabilities and related activities into the overall campaign plan at a particular level of command. Care should be taken to tailor the size and structure of the cell to meet the needs of the mission and Commander's Intent. Cells that are too large and over-manned can be just as detrimental to the success of the mission as those that are undermanned. There are typically 3-6 resident members in a CC IO Cell. During deliberate planning, the IO cell chief will convene from time to time an Information Operations Working Group (IOWG). The purpose of the IOWG is discussed later in this chapter. Below shows the doctrinal view of a Joint IO cell.



The size and composition of the IO Cell is determined by the scope of the operation. The J3 must decide on which members will be resident (permanent) on the cell and which will be non-resident (on-call). Lessons learned from Operation ALLIED FORCE called for the re-organization of the IO cell into functional areas. The following graphic shows a possible IO cell organization during crisis.

IO Cell During Crisis



4

The Commander normally assigns responsibilities for IO to the Operations Officer (or J3). To assist the J3 in exercising joint IO responsibilities, the J3 may also appoint an IO officer as the IO Cell Chief. Some of the generic responsibilities of the IO officer and IO cell resident members are listed below.

The J3, by doctrine, is responsible for integrating and synchronizing IO with all other elements of the operation. To assist the J3 in exercising joint IO responsibilities, the J3 usually appoints an IO officer as the IO Cell Chief. Some of the generic responsibilities of the IO officer and IO cell resident members are listed below.

Information Operations Cell Chief

Plans, coordinates, and integrates IO capabilities and activities among the various subordinate elements of a command. A key to the success of the IO Cell is the success of the IO officer in integrating the commander's guidance into planning meetings and directly facilitating coordination between the components. Additional specific responsibilities include:

- Coordinating the overall IO effort for the command.
- Coordinating IO issues within the CC's staff and counterpart IO planners on the component staffs.
- Coordinating IO defensive and offensive concepts to support the commander's intent and concept of operations.
- Establishing priorities to accomplish IO objectives.
- Determining the availability of resources to carry out IO plans.
- Recommending tasking to the J3 for joint organizations that plan and supervise the various capabilities and related activities to be utilized. Consolidated J3 tasking ensures efficiency of effort in planning and executing integrated IO.
- Serving as the primary "advocate" for IO targets nominated for attack throughout the target nomination and review process established by the commander.
- Coordinating intelligence and assessment support to IO.
- Coordinating IO inputs from joint centers and agencies.
- Coordinating liaison with outside organizations such as the Joint Information Operations Center (JIOC), Joint Warfare Analysis Center (JWAC) etc.
- Assist the J3 in integrating STO capabilities.

IO Cell Responsibilities

Intelligence Support Team

- Serve as the IO point of contact for all IO related intelligence requirements.
- Provide the IO cell the following information (note that this list is not all inclusive):
 - Identify key adversary decision makers, both military and non-military. This may include human factors analysis studies.
 - Identify the adversary's information infrastructure and its critical vulnerabilities.
 - Identify the adversary's offensive IO capabilities and potential IO courses of action against the Joint Force.
 - Identify adversary IO vulnerabilities.
 - Provide Psychological Operations profiles of adversary countries and population groups.
- Serve as the IO red team cell chief during cell war games

Perception Management Team

- Provide dedicated IO planning support to the Joint Planning Group (JPG). Other planners (STO, CNO, OPSEC, Deception, etc.) will support as required.
- Develop an IO plan that supports the selected COA.
- Write, with input from everyone, the IO appendix to the Operations annex.
- During crisis, coordinate with appropriate staff element (such as the Joint Fires Element) to provide daily input into the targeting objectives and guidance promulgated to the components.
- Develop Measures of Effectiveness that support the accomplishment of stated IO objectives. In conjunction with the J2 and J3 campaign analysis cell (if used), conduct assessment of the impact of IO throughout the course of the operation.
- Host the daily IOWG

Physical Effects Team

- Develop a target plan (both non-lethal and lethal) that will support the accomplishment of the IO objectives. Integrate all elements and related activities into the plan.
- Responsible for ensuring IO targets and activities are integrated into the joint targeting process. This includes:
 - Nominate targets as required for attack through the appropriate J3 staff element (such as the JFE).
 - Nominate targets as required for inclusion on the restricted and prohibited target lists to the appropriate J2 or J3 staff element.
 - Develop IO input to the daily Joint Targeting Coordination Board.
 - Assist in developing MOEs.

Computer Network Operations Team

- Coordinate CNO actions that will support the overall JF concept of operations.
- Assist the J6 and other staff sections a consolidated list of information networks and activities that need to be protected
- Coordinate with higher headquarters for CNA options. De-conflict and integrate any planned CNA actions with other elements of the operation.

Special Technical Operations

- Coordinate, de-conflict and synchronize any planned STO with all other elements of the operation.

Watch Standers

- Stationed in the Joint Operations Center (JOC).
- Monitor activities in the JOC that could impact on the IO plan and report them to the IO cell.
- Consolidate IO input to SITREPs as required and provide them to the JOC chief.
- Perform duties as required by the JOC chief.

PSYOP Planner

- Integrates PSYOP planning with other perception management activities.

- Member of the Perception Management Team.

Public Affairs Planner

- Member of the Perception Management Team.
- Coordinates media interface ensuring that press releases, etc. do not conflict with the JF Commander's intent.
- Provides IO cell with analysis of open source media with regards to the current operation.

Civil Affairs Planner

- Member of the Perception Management Team.
- Provides the IO cell updates on what the IO, NGO and PVO organizations are doing in the AOR.
- Ensures consistency of CA activities in support of the IO objectives.

Information Coordination Board

The purpose of the Information Coordination Board (ICB) is to synchronize all the information flowing within the headquarters and subordinate elements, ensuring all the information released from the headquarters are complementary of each other, in consonance with the overall commander's intent and information themes, and focused on the critical audiences. This optional board is convened by the J3 upon the recommendation of the IO cell chief.

Usually, chaired by the J3 (or representative) with participation from J2, J3, J7, PA, IO (especially PSYOP), SJA, Political-Military Section, and political-military advisor (POLAD). This board should meet as required – initially on a daily, scheduled basis.

Information Operations Working Group (IOWG)

The purpose of the Information Operations Working Group (IOWG) is to coordinate the Information Operations activities across the staff, and synchronize activities and actions with higher headquarters and the components. The IO cell chief needs to establish the requirement for an IOWG and ensure it is included the Joint Force staff battle rhythm. By including the IOWG into the battle rhythm, it by necessity will be de-conflicted with other staff meetings and will facilitate attendance by LNOs and other members of the staff.

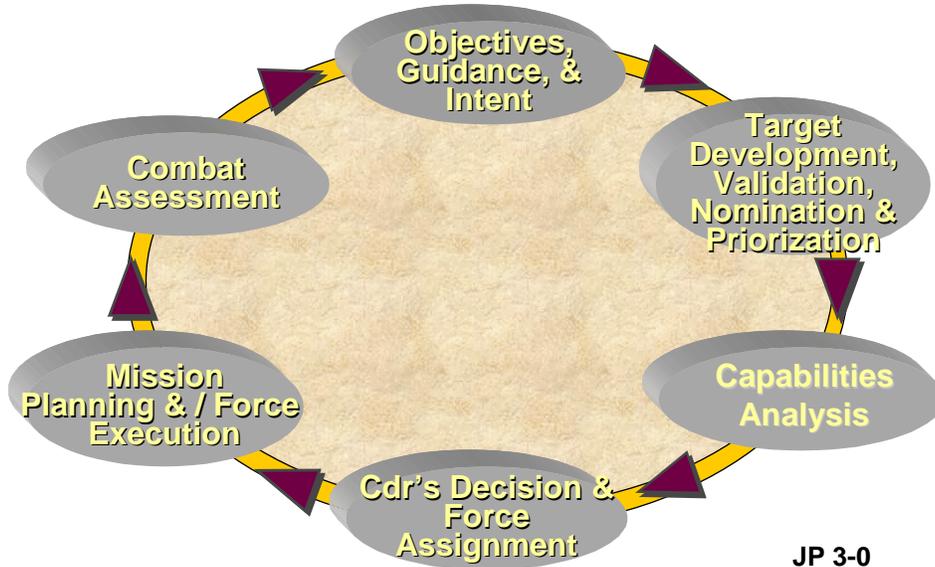
The placement of the IOWG into the staff battle rhythm is predicated on when the higher headquarters IO VTC (if any) is scheduled, as well as when the deliverables are due to other staff sections or components.

The IO cell chief with the approval of the J3 sets the agenda of the IOWG. A typical agenda is a follows:

- Current Operations Update
- Future Operations Update
- Future Plans Update
- Review Status of Previous Taskers
- Review of actions of the IO cell by discipline
- Review of actions by higher headquarters and components
- Determination of future IO cell actions

The deliverables of an IO cell vary. Normally, during a planning evolution, the focus will be supported the J5 or Joint Planning Group (JPG). During crisis, the IO cell will be responding to variety of internally and externally generated tasking.

Targeting Integration



The joint targeting process (See above) is the process used by the Information Operations Cell.

Methodology

The joint targeting process as described in Joint Pub 3-09 and Joint Pub 3-0 is a six-step process: Objectives, Guidance and Intent, Target Development, Validation, Nomination, and Prioritization, Capabilities Analysis (Weaponeeing), Commanders Decision and Force Assignment, Mission Planning and Force Execution, and Combat Assessment. The associated functions of each step are accomplished at a variety of levels, from national organizations down to tactical units. The primary responsibility for targeting at the operational level of war resides with the JF. The JFC's objectives, guidance and intent direct and focus operational planning and targeting to support the concept of operations.

- a. **Objectives, Guidance and Intent.** The development and dissemination of objectives, guidance and intent marks the first step in the target process and is arguably the most critical. Objectives and guidance must identify what is to be achieved and under what conditions and parameters the end is pursued. That is, objectives and guidance must clearly spell out the task, purpose and measurable endstate of targeting process to the overall campaign plan. An objective must be observable, attainable, and measurable. Part and parcel with the development of objectives, the IO planner must develop Measures of Effectiveness (MOE) and indicators to guide the intelligence collection effort and combat assessment when the plan is executed. Lastly the JFC's Intent is continually checked to ensure that the objectives and guidance match the end state of the operation.
- b. **Target Development, Validation, Nomination, and Prioritization.** During the first part of this process the target development is done by a collaborated operations, intelligence and interagency team that identifies a variety of "effects based" options to the warfighter. Effects based targeting is the method that identifies the most efficient set of targets that produces a specific effect consistent with the JFC's objectives. Targets can be physical (fixed or mobile), electronic (e.g. links between communications systems) or perception (influencing key decision makers). Targets nominated for inclusion on the Joint Target List (JTL) need to be validated by the Intelligence Community and the Supported CC. Once targets are validated, the IO cell for attack can nominate them. Normally, physical targets are forwarded to the Guidance, Apportionment and Targeting (GAT) cell located at the

Joint Air Operations Center (JAOC) where they are “racked and stacked” in accordance with the priorities set forth by the JFC. During this meeting, all of the component and JF target nominations are rank-ordered in accordance with CJF targeting guidance and priorities. The cut line (a staff estimate of which targets are mostly likely to be attacked based upon the number of fully mission capable aircraft available for that ATO day) is then established in accordance with the JF Commander’s apportionment recommendation. The end result of this meeting is a draft Joint Integrated Prioritized Target List (JIPTL). This list of targets is normally forwarded to the Joint Force Headquarters to be reviewed by the Joint Targeting Coordination Board (JTCB) for approval. The JTCB is a decision making board, normally chaired by the Deputy Joint Force Commander. The IO cell chief and PSYOP LNO should have a seat at the table for the JTCB. The JTCB Chairman normally will ask the board members for comments concerning the JIPTL and then takes a voice vote of concurrence or non-concurrence. To ensure this is a meaningful vote, it is essential the component liaison elements (including the IO rep) at the JAOC keep their commanders, staffs, and JTCB board members aware of the status of their target nominations as the GAT process progresses. The JFACC staff (Combat Plans Division) uses the approved JIPTL to develop the Master Air Attack Plan (MAAP) and then to issue the Air Tasking Order (ATO).

- c. **Capabilities Analysis (Weaponneering).** Weaponneering (or weapons pairing) is the process whereby the number and type of munitions needed to achieve a specific effect against a target is determined. Weaponneering takes into account target vulnerabilities, weapons effects and reliability, delivery accuracy, delivery conditions, and damage criteria. The process of weaponneering is equally applicable to the employment of both lethal and non-lethal weapons.
- d. **Commanders Decision and Force Assignment.** During the force assignment step, lethal and/or non-lethal forces are selected for a particular joint attack. Component commanders – in accordance with the JFC’s guidance – conduct force application planning to fuse target, weapon system, munitions, and non-lethal force options together. This step results in the coordinated selection of forces and associated weapons systems or platforms.
- e. **Execution.** During the execution planning/force execution step, component staffs prepare input for and support the actual tasking, construction and subsequent execution of missions for weapons systems. The input includes all data concerning the target, the weaponneering calculations, employment parameters, and tactics.
- f. **Combat Assessment.** During this step, component staffs determine whether or not the effectiveness that particular cycle’s joint fires. There are three components to combat assessment: battle damage assessment (BDA), munitions effectiveness assessment (MEA), and re-attack recommendations. MEA concerns the actual performance of the weapon during the attack. BDA consists of three phases: Physical, functional and target system analysis. Phase I BDA, or physical damage assessment, is the initial assessment on whether or not the munition hit the target. This accomplished by looking at the Cockpit video, imagery analysis and pilot debriefing. Phase II BDA, or functional damage assessment, is the combining of Phase I BDA with other intelligence reports to determine if the activity or installation is still functioning. Phase III BDA, or target system analysis, is the intelligence assessment on the impact of the target system (e.g. IADS, telecommunications, POL) as a whole. Finally staffs prepare re-attack recommendations after analyzing desired effects against BDA and MEA.

Finally, the IO cell needs to be aware that not all IO activities will fit neatly into the ATO time line. For example, Computer Network Attack (CNA) and Special Technical Operations (STO) will certainly need to be integrated and synchronized with the ATO process. CNA and STO have their own timelines and approval processes. Additionally, PSYOP product approval and dissemination can take anywhere from a few days to weeks to implement.

Lists related to targeting

- Joint Target List (JTL) – The master target list of all targets in the area of operations. Normally maintained by the J2.

- Prohibited Target List – Targets such as churches, schools, hospitals, or special interest facilities, which planners do not want to target or damage.
- Restricted Target List – Targets that cannot be attacked unless coordinated with the established agency or component. Typical type targets include communications sites that have Intelligence Gain / Loss (IGL) concerns and fixed facilities that the friendly force intends to use in the future and does not want struck.
- Joint Integrated Prioritized Target List (JIPTL) – A prioritized list of targets that need to be acted on to meet the JFC's overall objective.
- High Payoff Target List (HPTL) – Categorized and prioritized list, including lethal and non-lethal means, sent to components as guidance.
- Joint Restricted Frequency List – Deconflicts friendly use of the RF spectrum.

External Augmentation

Resident expertise on the IO staff can always use augmentation. As such, knowledge of organizations external to your staff can provide that expertise. The following is a short list of some of the more significant organizations available to JTFs.

- **Joint Information Operations Center (JIOC).** The JIOC supports the integration of OPSEC, PSYOP, military deception, EW and destruction throughout the planning and execution phases of operations. They also provide direct support to unified commands, JTFs, functional and service components, and subordinate combat commanders. Manning includes specialized expertise in C2 systems engineering, operational applications, capabilities and vulnerabilities.
 - **URL:** <http://www.jiolink.jioc.smil.mil>
- **Joint Warfare Analysis Center (JWAC).** The JWAC provides support for analysis of engineering data and scientific data. This data is also integrated with intelligence data to support targeting.
 - **URL:** <http://www.jwac.jfcom.smil.mil>
- **Joint Program Office for Special Technology Countermeasures (JPO-STC).** JPO-STC has the ability to assess a command's infrastructure dependencies and the potential impact on operations resulting from disruptions to key infrastructure components.
 - **URL:** <http://www.jpo-stc.nswcdd.navy.smil.mil/>
- **Joint COMSEC Monitoring Activity (JCMA).** JCMA provides communications security monitoring and analysis support.
 - **URL:** <http://www.nsa.smil.mil/producer/jcma/>
- **Joint Spectrum Center (JSC).** The JSC maintains expertise in the following areas: spectrum planning, electromagnetic compatibility/vulnerability, electromagnetic environmental effects, information systems, modeling and simulation, operations support, and system acquisition to provide spectrum-related services to the CCs, military services and other governmental organizations.
 - **URL:** <http://jsc.js.smil.mil>
- **Joint Communications Support Element (JCSE).** The JCSE is a JCS asset designed to provide tactical / operational communications support to a JF. They also provide planners to assist to developing communications structures.
 - **URL:** <http://jcse.nmcc.smil.mil/>
- **USJFCOM Joint Warfighting Center (JWFC).** USJFCOM's JWFC, in conjunction with the Joint Training, Analysis, and Simulation Center (JTASC), provides training support to CC staffs and Joint and Combined JF's. In addition to providing Computer Assisted Simulation exercises in support of warfighters, they also provide deployable training team support to real world operations.
 - **URL:** <http://www.jwfc.jfcom.smil.mil/>

- **Joint Command, Control and Information Warfare School (JCIWS), Joint Forces Staff College.** The JCIWS offers three courses that are essential for educating the personnel of an IO Cell. The “Joint Command, Control, Communications, Computers and Intelligence Staff and Operations Course” (JC4ISOC) covers topics such as: fundamentals of command and control, fundamentals of communications, national emergency management system, national military command organization, orbital mechanics, C4I for the warrior, and the Global Command and Control System (GCCS). The Joint Information Warfare Staff and Operations Course (JIWSOC) approaches IO as a broad, integrating strategy in accordance with Joint Publication 3-13 (Information Operations). The course focuses on national IO organization, offensive and defensive information warfare, critical infrastructure protection, IO planning and execution, computer network attack, Information Assurance, and service component IW capabilities. The Joint Information Operations Planning Course (JIOPC) offers an in-depth look at IO planning using the Joint IO Planning Process developed by the JIOC.
 - **URL:** <http://www.jfsc.ndu.edu/jciws/jciws.htm>
- **U.S. Strategic Command (USSTRATCOM)** – USSTRATCOM provides Computer Network Defense (CND) and Computer Network Attack (CNA) support for the DoD. The CND mission is executed through the JTF for Computer Network Operations (JTF-CNO). Each military service has a component Computer Emergency Response Team (CERT) subordinate to the JTF-CNO.
 - **URL:** <http://www.stratcom.smil.mil>
- **Air Force Information Warfare Center (AFIWC).** AFIWC develops, maintains and deploys information warfare/command and control warfare capabilities in support of operations, campaign planning, acquisition and testing. Providing technical expertise for computer and communications security, AFIWC is the focal point for tactical deception and operations security training. AFIWC provides the U.S. Air Force component of the JTF-CNO.
 - **URL:** <http://www.afiwk.aia.kelly.af.smil.mil>
- **1st Information Operations Command (Land) [1IOC].** 1IOC provides Information Operations support to Army units and Army headquarters designated as JF headquarters. Its focus is on field support teams that deploy worldwide to support U.S. Army operations. 1IOC also provides the Army component of the JTF-CNO.
 - **URL:** <http://www.1ioc.army.smil.mil>
- **Fleet Information Warfare Center (FIWC).** FIWC provides IW support to Navy and Marine Corps units worldwide. Its focus is providing training support and personnel augmentation to the IW staff of aircraft carrier battle groups and monitoring U.S. Navy computer networks.
 - **URL:** <http://www.fiwk.navy.smil.mil>

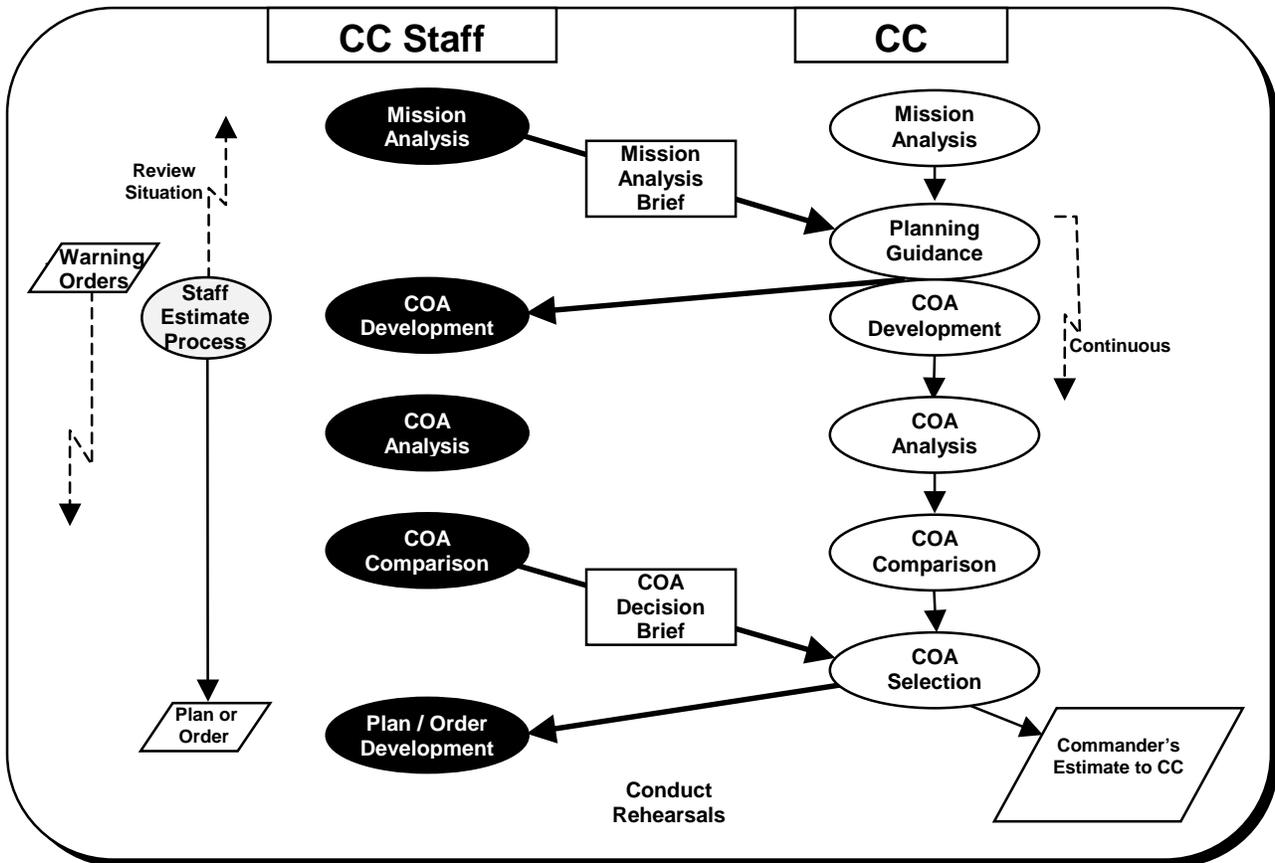
Chapter III – Planning Joint Force Information Operations: Integrating Information Operations in the Staff Planning Process

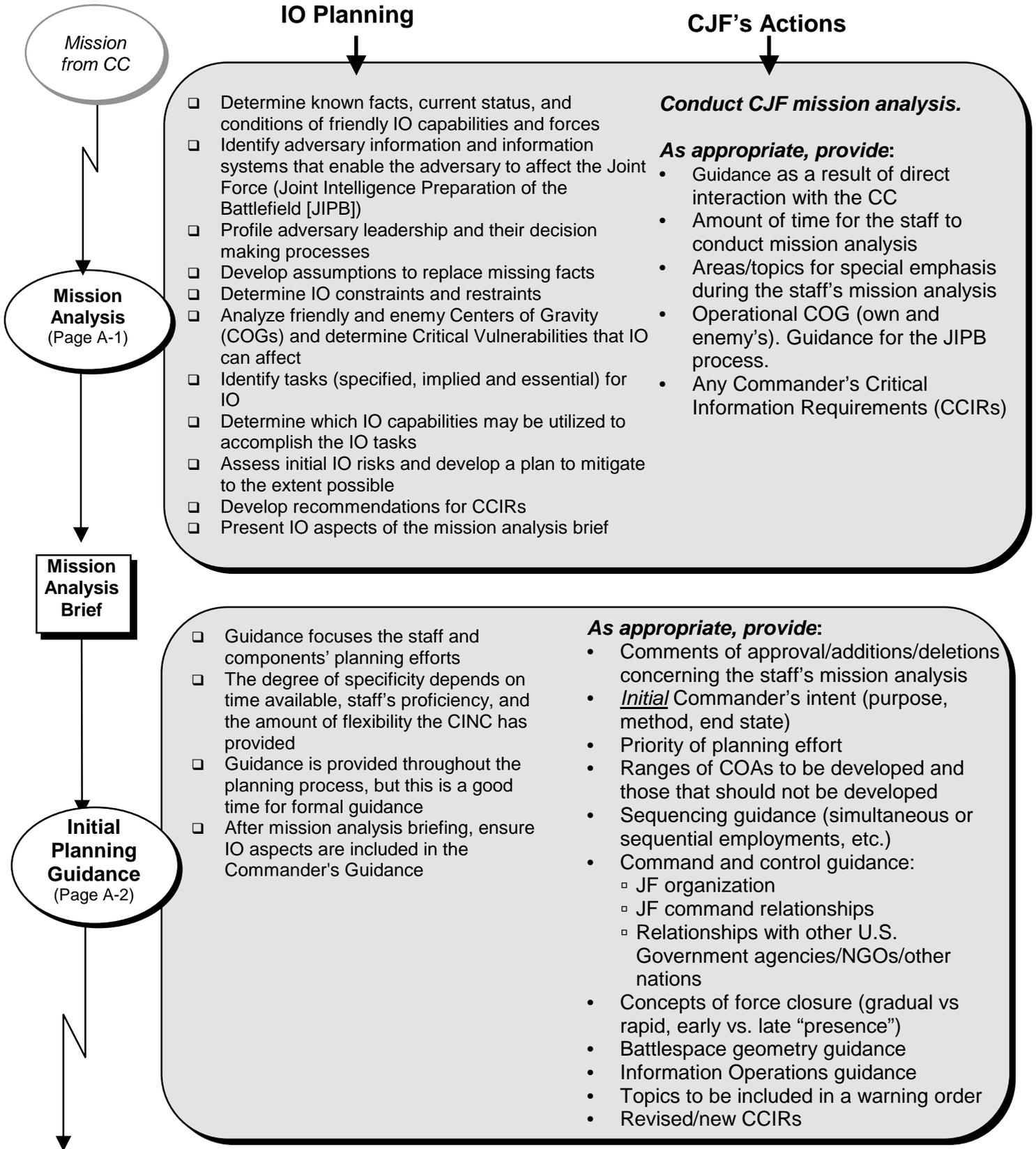
*“Master the mechanics and techniques; understand the art and profession; and
be smart enough to know when to deviate from it.”*

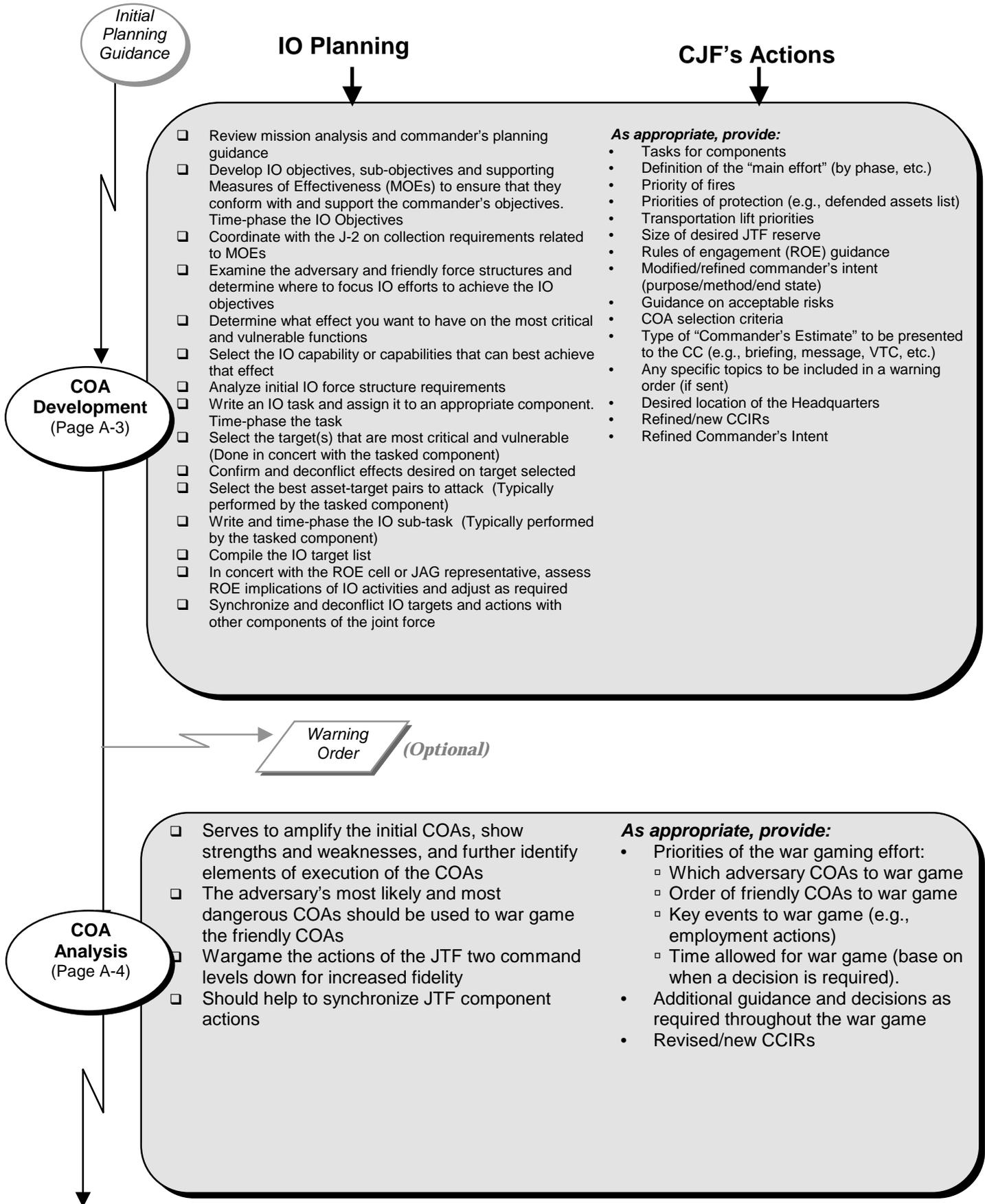
GEN Zinni, CENTCOM

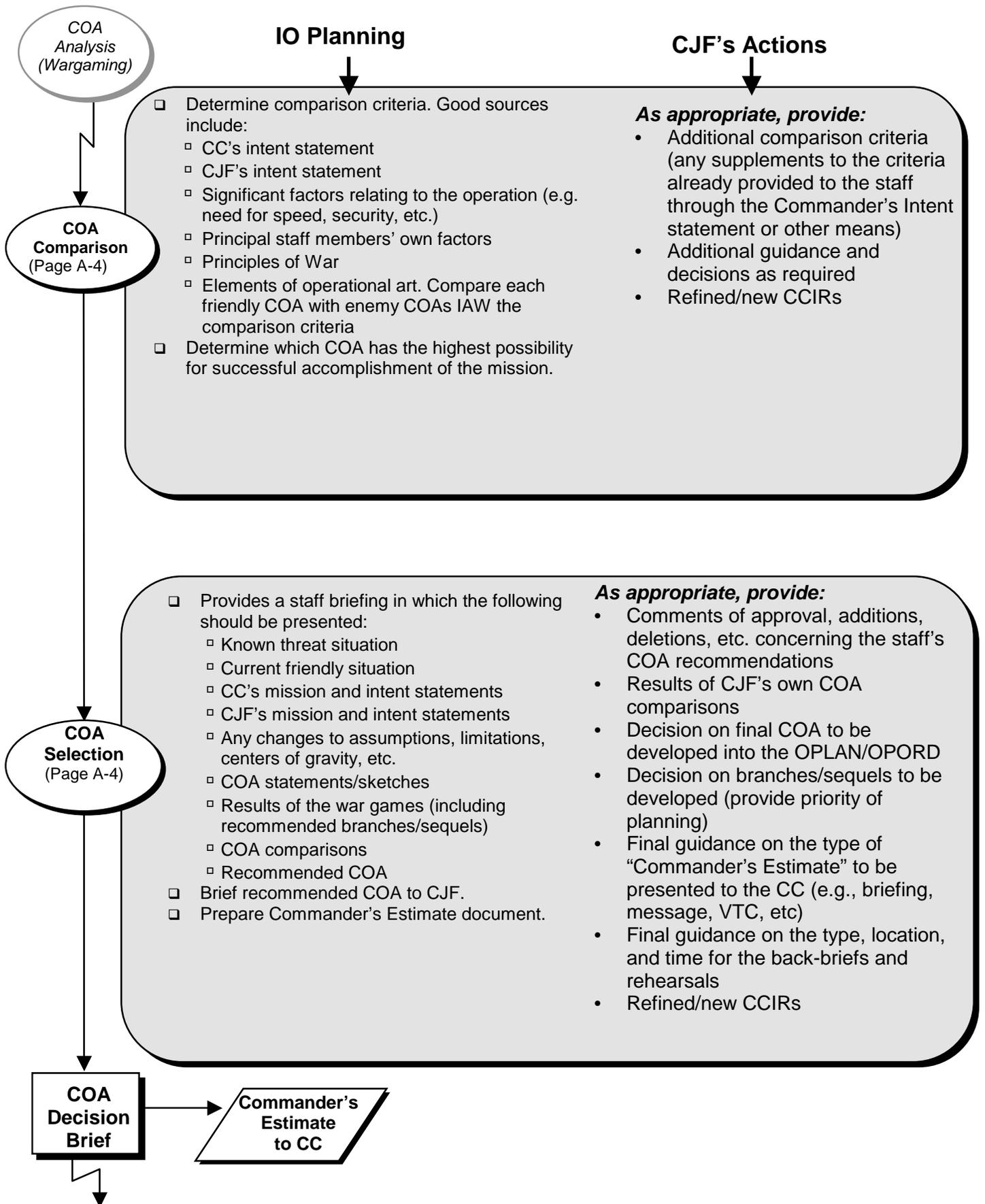
Information Operations Planning

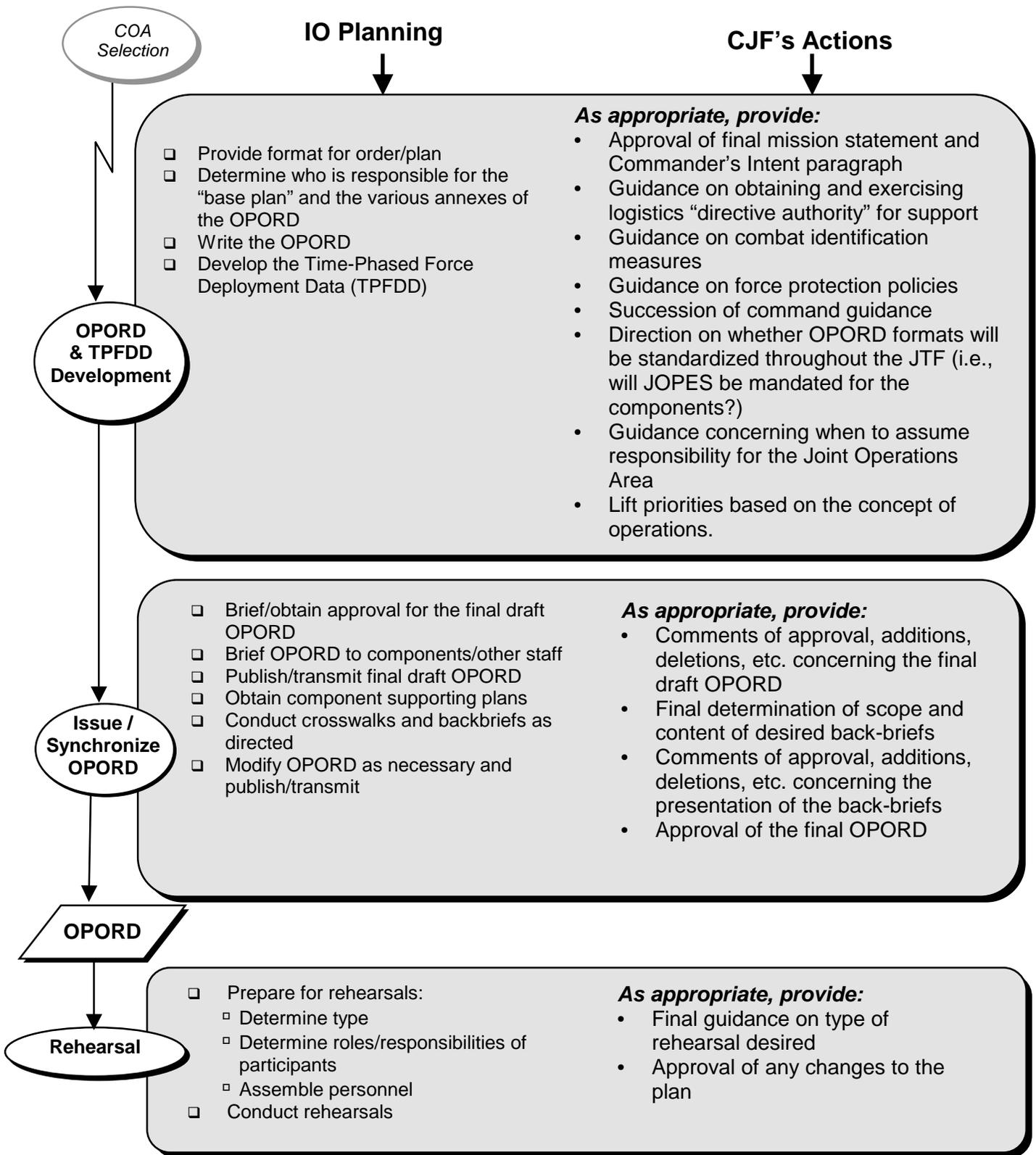
The figure below depicts some of the “mechanics and techniques” of joint planning which GEN Zinni refers to in the above quote. This is a dynamic process that requires close cooperation and involvement between the CC and staff and is proportionally more efficient with greater Commander involvement. This process is used in crisis action planning by a JF and interfaces with the strategic level Crisis Action Planning (CAP) process used by the CC and the SECDEF. **To be successful, IO planning must be integrated into this process.** The following pages provide a summary of how IO planning should parallel the overall JF planning process. Annex A provides more details about IO planning (including planning considerations for each IO capability and related activity).











Intelligence Support

Intelligence support is critical to the planning and execution of an effective IO campaign. Intelligence support to IO may require significant lead-time; consequently, early coordination must be established between the IO cell and the J2 staff. Intelligence data produced by the joint Intelligence Preparation of the Battlespace (IPB) process must be readily available on a near real-time basis. Intelligence information systems collect, process, disseminate, and display data that is essential to the IO cell. All members of the IO cell should understand the sources and methods of intelligence support to fully utilize the capabilities of the J2 staff and the intelligence community.

Offensive Information Operations

Intelligence to support offensive IO requires: knowledge of the technical requirements of a wide array of an adversary's information systems; knowledge of political, economic, social, and cultural influences; the ability to develop templates used to portray the battlespace and refine targets and methods for offensive IO courses of action (COAs); an understanding of the adversary's decision-making process; an in-depth understanding of the biographical background and psychological makeup of key adversary leaders, decision-makers, communicators and their advisors to include motivating factors and leadership style; knowledge of the area of responsibility/joint operations area's geographic, atmospheric, and littoral influences on adversary and friendly operations; and knowledge of offensive IO measures of effectiveness (MOE) in order to conduct effective assessment of the effectiveness of friendly offensive IO.

Defensive Information Operations

Intelligence to support defensive IO requires: knowledge of an adversary's intelligence interests and methods of intelligence collection; an understanding of the adversary to friendly information and information systems posed by a particular adversary, including their intent and their known and assessed capabilities; and an ability to provide indications and warning of impending offensive information operations attacks by an adversary. The following is a sequential overview of intelligence support to IO targeting:

- Identify system's value, use, flow and vulnerabilities
- Identify specific targets
- Develop target set
- Determine most effective IO capabilities against that target
- Predict the consequences
- Perform a technology cost/benefit analysis for the IO tool to be used
- Monitor friendly Information Operations
- Establish assessment/feedback mechanisms
- Evaluate the outcome
- Provide battle damage assessment (BDA) for the IO

Chapter IV – Integrating Information Operations in JOPES Deliberate/Crisis Action Planning/Execution on a Unified Command Staff

This chapter is intended to be a basic introduction of the Joint Operational Planning and Execution System (JOPES) using an IO-related example. It is based on materials from the JIWSOC IO Planning class.

We will start with a brief discussion of theater engagement planning as an introduction. Then we will spend most of the chapter focusing on IO in Deliberate Planning. Then we will look at Crisis Action Planning only as it differs from Deliberate Planning.

Introduction

In this section, we will cover

- Basic IO policy
- Applicability of IO to theater engagement
- Provide some useful principles
- The “Strategy-to-Task” methodology

These slides are from the JIWSOC IO Planning Class. Exercise content of the following slides is for instructional use only.



DoD Policy on IO Planning

Policy: (U) DoD activities shall be organized, trained, equipped, and supported to plan and execute IO

-- DoD Directive S-3600.1

Goal: (U) The goal of IO is to secure peacetime national security objectives, deter conflict, protect DoD information systems, and to shape the information environment.

-- DoD Directive S-3600.1

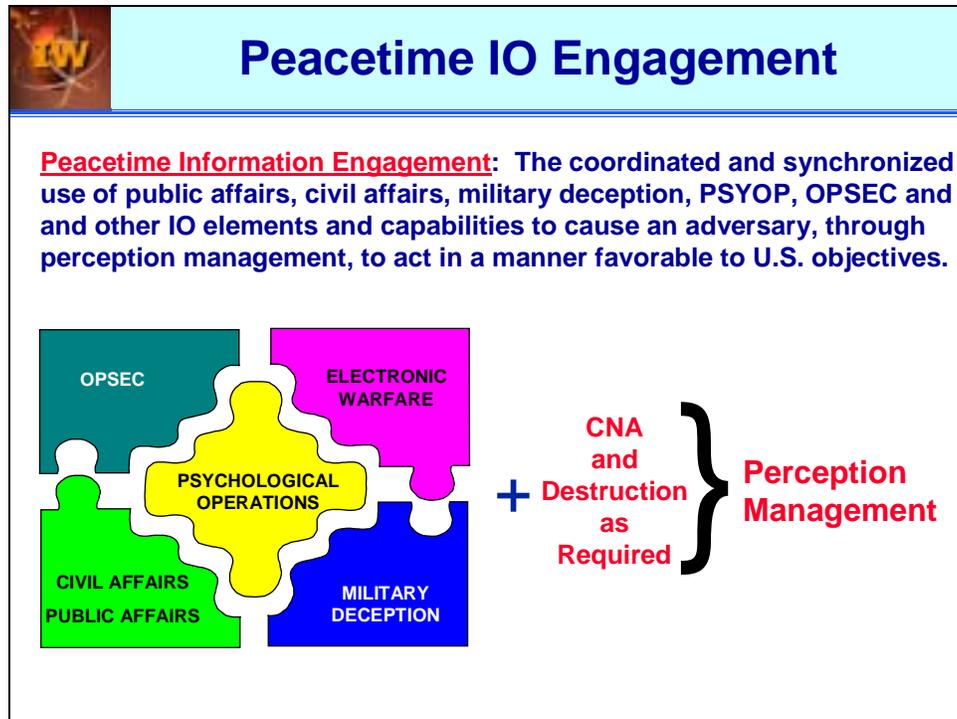
New DoD Directive 3600.1 is out for signature



Why do we plan for IO?

DoD Directive S-3600.1 *Information Operations* is the basic policy document for IO in the DoD. It directs us to plan IO for the goal shown here. IO, by its nature, lends itself to peacetime engagement. It has therefore been incorporated into the Theater Security Cooperation Plans of the Regional CCs.

As of the date of publication, the revised directive is still out for review.

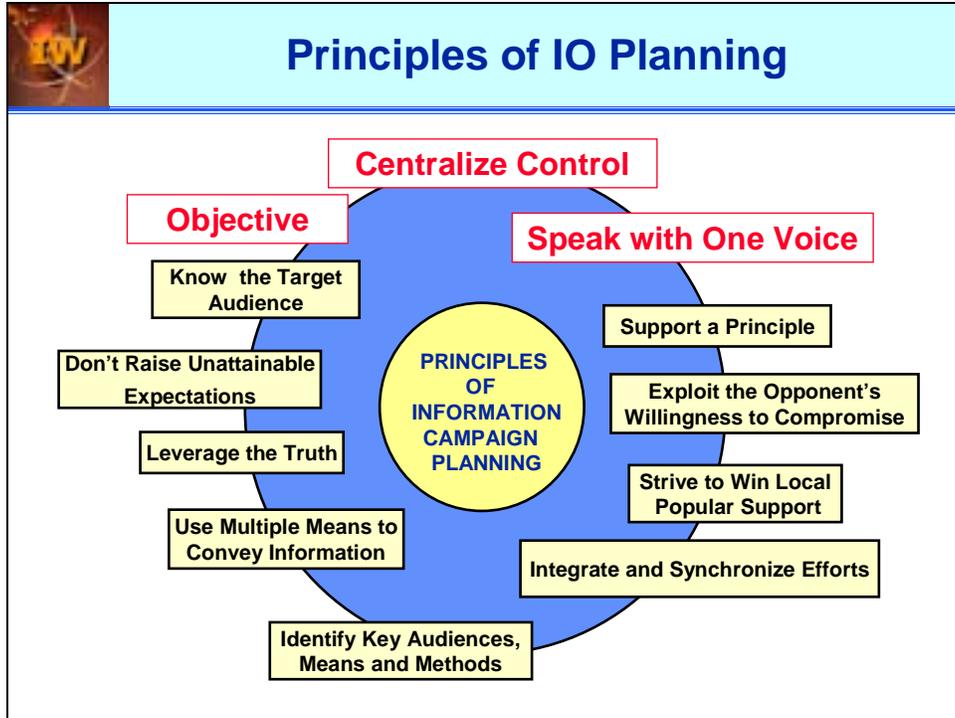


Peacetime IO Engagement

Peacetime Information Engagement: The coordinated and synchronized use of public affairs, civil affairs, military deception, PSYOP, OPSEC and other IO elements and capabilities to cause an adversary, through perception management, to act in a manner favorable to U.S. objectives.

The diagram illustrates the components of Peacetime Information Engagement. It features five interlocking puzzle pieces: OPSEC (teal), ELECTRONIC WARFARE (pink), PSYCHOLOGICAL OPERATIONS (yellow), CIVIL AFFAIRS and PUBLIC AFFAIRS (green), and MILITARY DECEPTION (blue). These pieces are combined with CNA and Destruction as Required, indicated by a plus sign and a bracket, to result in Perception Management.

This definition of “peacetime information engagement” was in one of the early draft versions of JP 3-13, but was not included in the final version. We have retained it because of the importance of IO in peacetime engagement. As you may surmise, CNA and Destruction are not key players in peacetime due to legal constraints.



These are non-doctrinal principles of IO planning that we've developed through the school of hard knocks with much input from CC IO cells. The three highlighted principles are key to successful IO. Centralized control is key. Speaking with one voice is the whole idea behind IPI and PDD-68. As you may remember, objective is a principle of war as espoused by Clausewitz. Supporting a principle involves working with a religious, moral or political theme appropriate with the target audience.



Plan Objective

“War plans cover every aspect of a war, and weave them all into a single operation that must have a single, ultimate objective in which all particular aims are reconciled.”

Carl Maria von Clausewitz

**STRATEGY-TO-TASK
PLANNING METHODOLOGY**

Under the principle of objective, all actions must ultimately support the objectives (desired end-state/vision) of the Commander. To ensure we adhere to this principle, the IO community has adopted a planning methodology called “Strategy-to-Task”. We will use this methodology extensively.



“Strategy-to-Task” Methodology

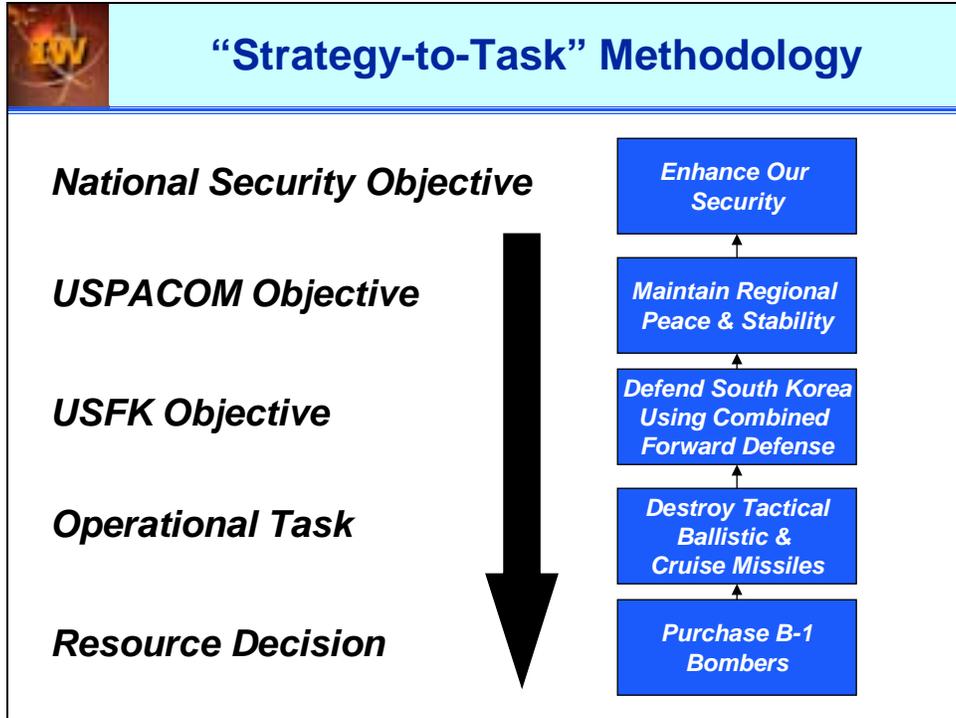
Developed at Rand in the late 1980s



Initially used to justify AF resource decisions by linking resources to operational tasks to national strategy

Concept gradually modified and used in planning

The Strategy-to-Task Resource Management framework, developed at RAND during the late 1980s, is a decision-support process for linking resources to the National Security Strategy. When used correctly, the framework links resource decisions to specific military tasks that require resources, which in turn are linked hierarchically to higher-level operational and national security objectives. The framework establishes the downward connection from strategies to programs and tasks, as well as the upward connection from tasks up through strategies.



The "Strategy-to-Task" methodology was built like this.

The initial derivation was in reverse, and started with the resource decision to purchase B-1 bombers. In a desire to link the bomber purchase to a national security objective, the authors looked for qualifying operational tasks for which the bomber was suited. An example is shown. This was then linked to a regional and then a CC objective. The CC objective was then linked to a national security objective. Building the chain from the bottom up ensured that the thought process irrevocably linked national security to the bomber purchase.

During the sales pitch for the bombers, the derivation of the linkages was presented from the top down. This example ends up with a resource decision. During planning, the process will frequently end with a task from the CC planners.



Both OPSEC and Deception can easily be forgotten as planning goes on. There should be an active planning element responsible for maintaining emphasis towards these important IO capabilities.

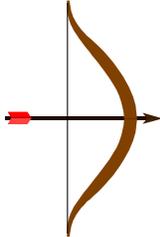
A graphic with a light blue header containing the title "Theater Security Cooperation Plan" in blue. Below the header is a white area with a bulleted list of points. In the top left corner of the graphic is a small logo with the letters "IO" in a stylized font.

- The Defense Planning Guidance (DPG) in **1997** directed the regional Combatant Commanders to document their peacetime engagement strategies looking out **five** years “down the road”
- Since extended to **seven** years
- This allows IO the proper / necessary lead-time to develop intelligence and do proper **Intelligence Preparation of the Battlespace (IPB)**
- The degree to which IO has been used varies from Combatant Commander to Combatant Commander – IO can help shape a theater and thereby avoid conflict
- Where we need work is finding a way to seamlessly link our **peacetime engagement** IO to the IO activities written into our CONPLANS and OPLANS.
- Renamed in 2002 from Theater Engagement Plan

Planning Basics

 **What Do Objective and Strategy Mean?**

- **Objective:**
 - Target
 - Aim
 - Goal
 - Ends
 - Answers the Question: **What**
- **Strategy:**
 - Plan
 - Method
 - Means
 - Answers the Question: **How**



 **Combatant Commander's Theater Strategy**

A Combatant Commander's strategy for attaining the the U.S. national objectives for a country or region may be stated in terms of IO as an integrating strategy.

Example: "I want to employ IO to help maintain **WHAT** stability during the elections in Mandura and to assist in the peaceful transition of government following the elections. We will accomplish this by:

- Informing the public of the benefits of a democratically elected government **HOW**
- Influencing potentially disruptive groups to refrain from interfering with the election
- Reassuring the public of continuity of government and public services during the post-election, transition period."

Now let's take a close look at the strategy-to-task planning methodology. In the example shown here, the CC, as allowed by doctrine, has chosen to use IO as the main effort in formulating his peacetime engagement strategy. In the example, the "what" portion is the CC's objective, and the "how" portion is his strategy.

What is a Concept of Operations?

- **CJCSM 3122.03 (JOPES Vol II):**
 - Summarizes how the commander visualizes execution of the operation from beginning to end
 - Describes how the IO will support the command's operational mission
 - Summarizes the concepts for supervision and termination of IO



What is a Concept of Operations?

- **Format:**
 - May be a single paragraph or divided into two or more paragraphs depending on operation complexity
 - When an operation involves various phases, the concept of operations should be prepared in sub-paragraphs describing the role of IO in each phase
 - The concepts for IO-offense and IO-defense may be addressed in separate sub-paragraphs



Integrating IO in Deliberate Planning

- IO is best suited to deliberate planning due to the occasionally long periods of time required to develop sources and access to an adversary's **information and information systems**



Plans

- Operation (OPLAN)
 - Any plan, except for the SIOP, for the conduct of military operations.
 - Prepared in either a complete format (OPLAN) or as a concept plan (CONPLAN)



Plans

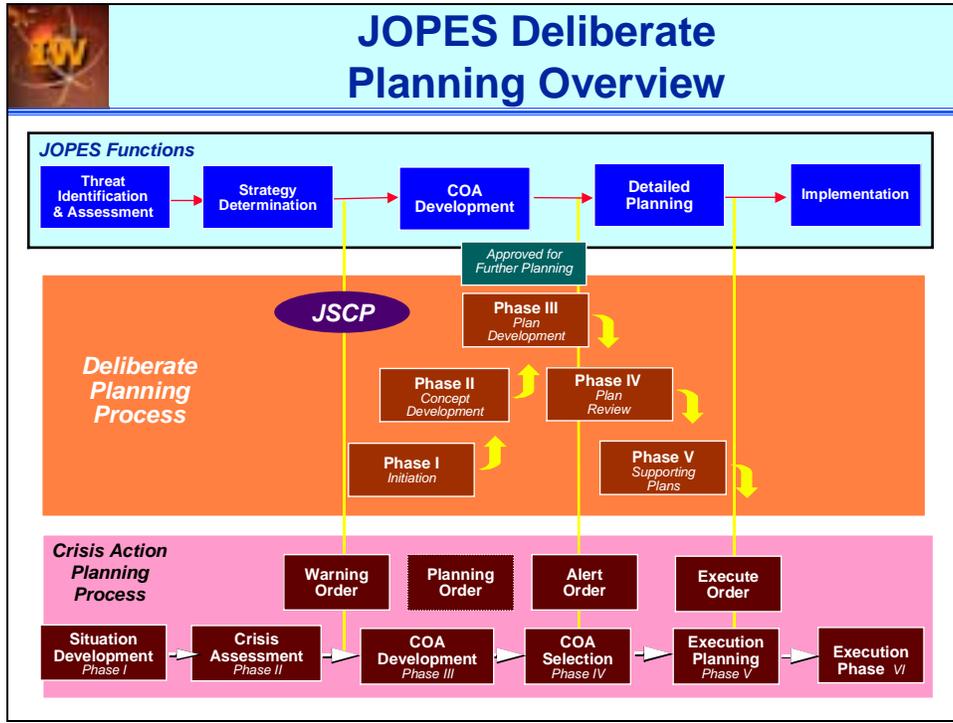
- **Functional**
 - Plans involving the conduct of military operations in a peacetime or permissive environment developed by combatant commanders to address requirements such as disaster relief, nation assistance, logistics, communications, surveillance, protection of U.S. citizens, nuclear weapon recovery and evacuation, and continuity of operations or other discrete tasks.



Plans

- **Concept (CONPLAN)**
 - An operation plan in an abbreviated format that would require considerable expansion or alteration to convert it into an OPLAN or OPORD. A CONPLAN contains the Combatant Commander's strategic concept and those annexes and appendices deemed necessary by the combatant commander to complete planning.
- **Contingency**
 - A plan for major contingencies that can reasonably be anticipated in the principal geographic sub-areas of the command.

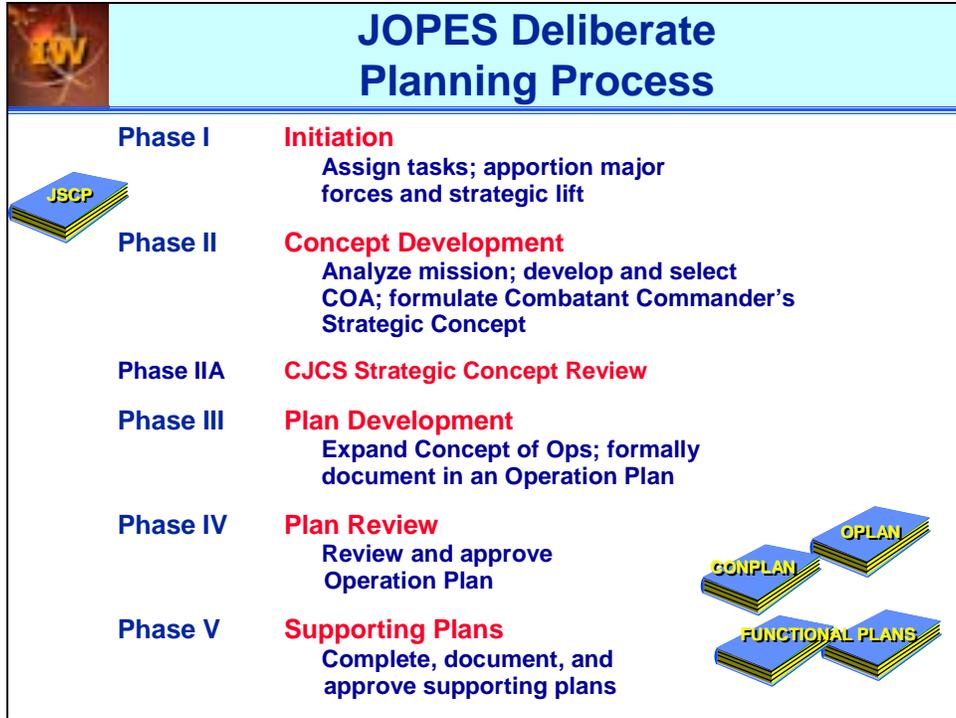
JOPES Deliberate Planning Process



1. The Joint Operations Planning and Execution System (JOPES). JOPES is the system used by DoD to plan and execute joint operations. JOPES consists of two planning systems, one for Deliberate (long-range) Planning and one for Crisis Action (time-sensitive) planning. Deliberate planning normally results in an operations plan (OPLAN), a concept plan (CONPLAN) with or without Time-Phased Force Deployment Data (TPFDD), or a functional plan. These plans must be approved by the Joint Staff and are then held until needed for execution or further planning. Crisis Action planning results in an operations order (OPORD) for immediate execution and may result in a series or related operations called a campaign plan. The definitions of the types of plans are found in Joint Publication 1-02.

2. Lead Time for IO Planning and Execution. Due to the sometimes-long periods of time required to develop sources and access to an adversary's information and information systems, IO is not well suited for Crisis Action Planning. Ideally, IO planning will be part of the CC's Theater Security Cooperation Plan (TSCP) for peacetime engagement activities. A good TSCP integrates IO into the CC's peacetime engagement strategy, thereby giving intelligence personnel and IO personnel sufficient lead-time to gain the necessary access and conduct the activities and coordination necessary for successful information operations.

3. Purpose of this section of the Joint IO Planning Handbook. This section provides a recommended approach for integrating IO planning into JOPES, on a step-by-step basis. The emphasis is on deliberate planning, for the reasons discussed in the preceding paragraph. The discussion herein is most applicable to a Unified Command IO Cell.



4. Deliberate Planning. The five phases of deliberate planning are shown here. The following discussion will look at each phase in detail.

4.a. Phase I of the Deliberate Planning process is the Initiation Phase. The deliberate planning process is normally initiated by the assignment of a mission to a unified command through the Joint Strategic Capabilities Plan (JSCP).

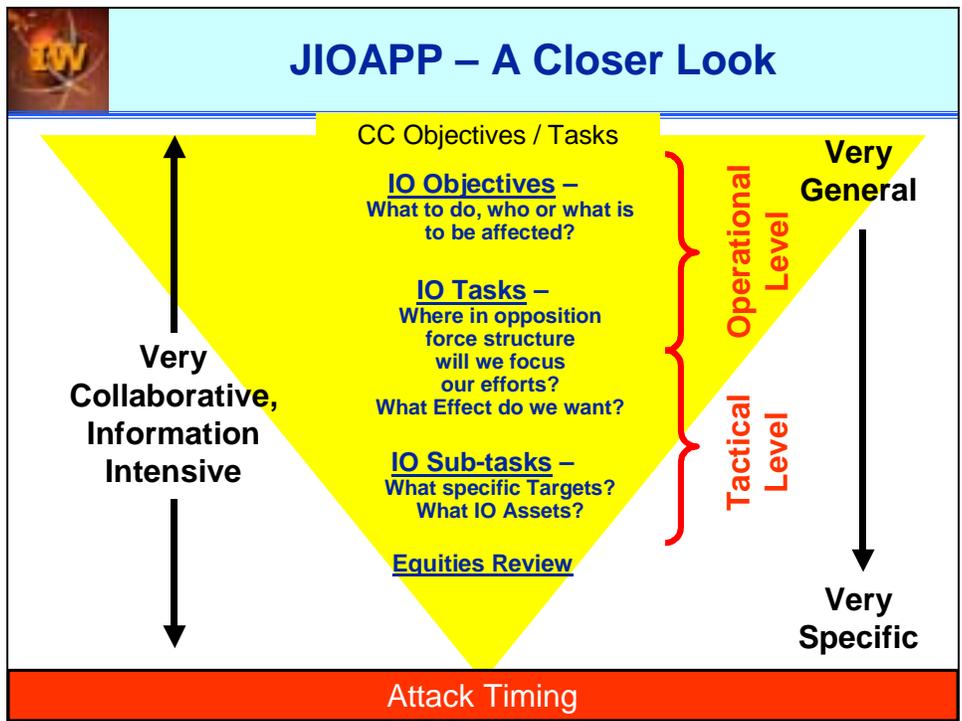
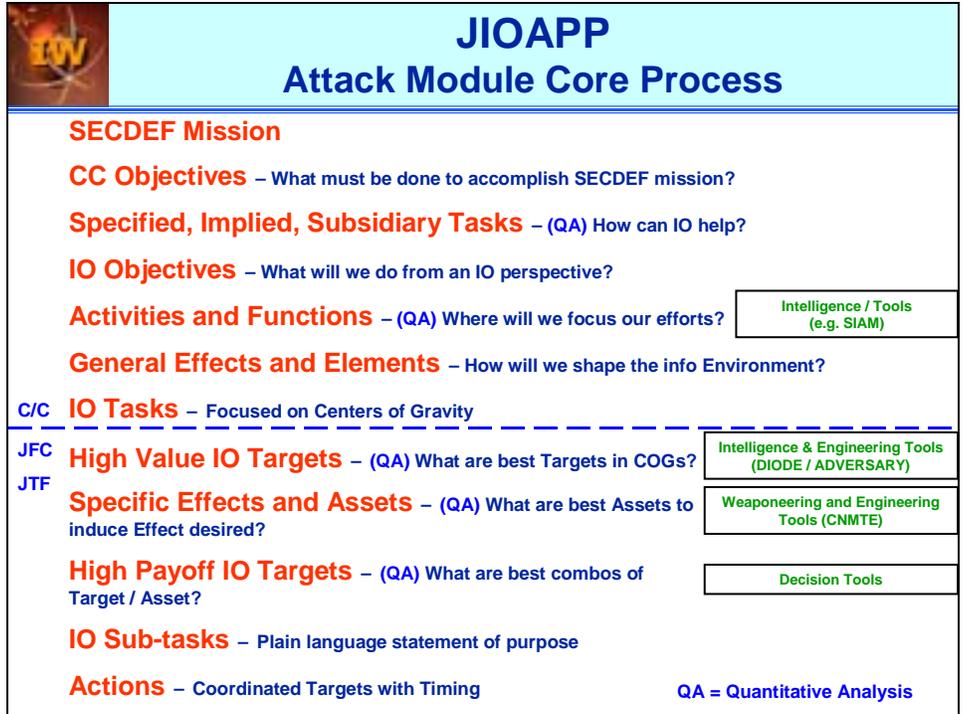
INFORMATION OPERATIONS PLANNING RELATED TO DELIBERATE PLANNING			
PLANNING PHASE	JOFFE	IO CELL PLANNING ACTION	IO PLANNING OUTCOME
PHASE I	Initiation	Notify IO cell members of planning requirements	N/A
PHASE II	Concept Development		
Step 1	Mission Analysis	IO cell identifies information requirements needed for mission planning	Seeking to gather/obtain required information
Step 2	Planning Guidance	IO cell assists in development of commander's IO planning guidance to support overall operational planning guidance	Commander's IO planning guidance for IO
Step 3	Staff Estimates	IO cell supports the development of intelligence, operations, and communications staff estimates	IO portion of staff estimates
Step 4	Commander's Estimate	IO cell assists in transforming staff estimates into the Commander's Estimate	IO portion of Commander's Estimate
Step 5	Commander's Concept	IO cell assists in the IO aspect of Commander's Concept as required	IO portion of Commander's Concept
Step 6	CACB Concept Review	IO cell assists in the IO aspect of CACB Concept Review as required	IO portion of operational concept approved by CACB
PHASE III	Plan Development	IO cell develops the complete IO plan and the plan for each of the IO elements in coordination with appropriate staff sections, operational units, and supporting agencies	Staff estimate and reference IO operations with relevant data
PHASE IV	Plan Review	IO cell facilitates/leads plan as necessary	Approved offensive and defensive IO operations
PHASE V	Supporting Plans	Subordinate units and supporting agencies prepare their own IO plans. IO cell coordinates/assists subordinate and supporting IO plan as necessary. Events TWDD supports IO plan	Completed subordinate and supporting agencies' supporting plans. IO plan supported by (TWDD)
CACB = Chairman of the Joint Chiefs of Staff IO = Information Operations TWDD = Two-Way Data and Deployment Data			

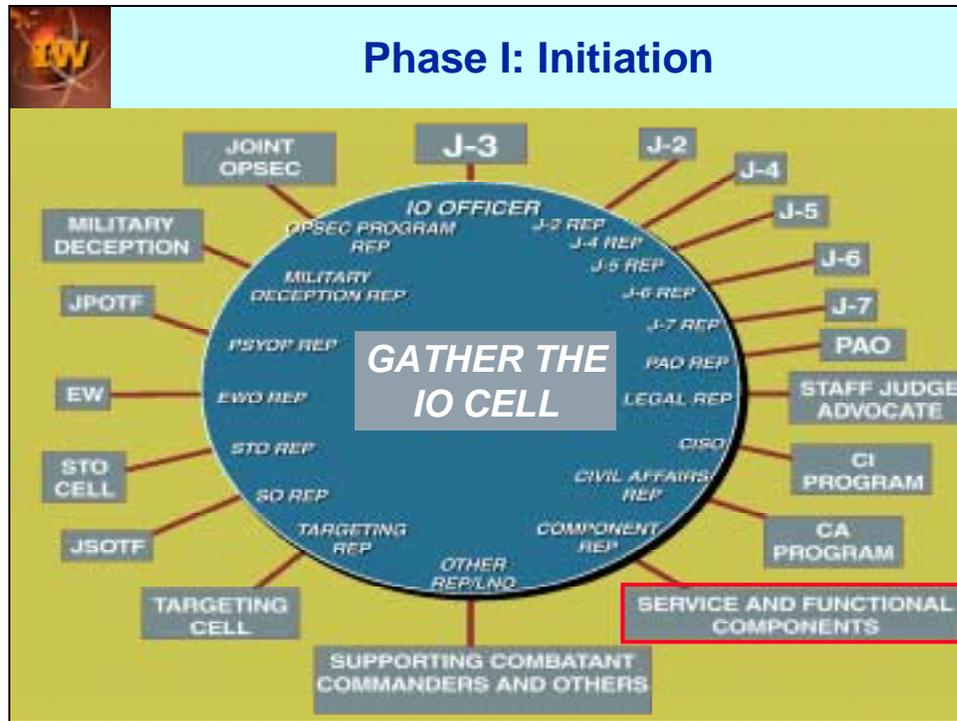
**IO
Deliberate
Planning**

**Joint Pub 3-13
Page V-7**

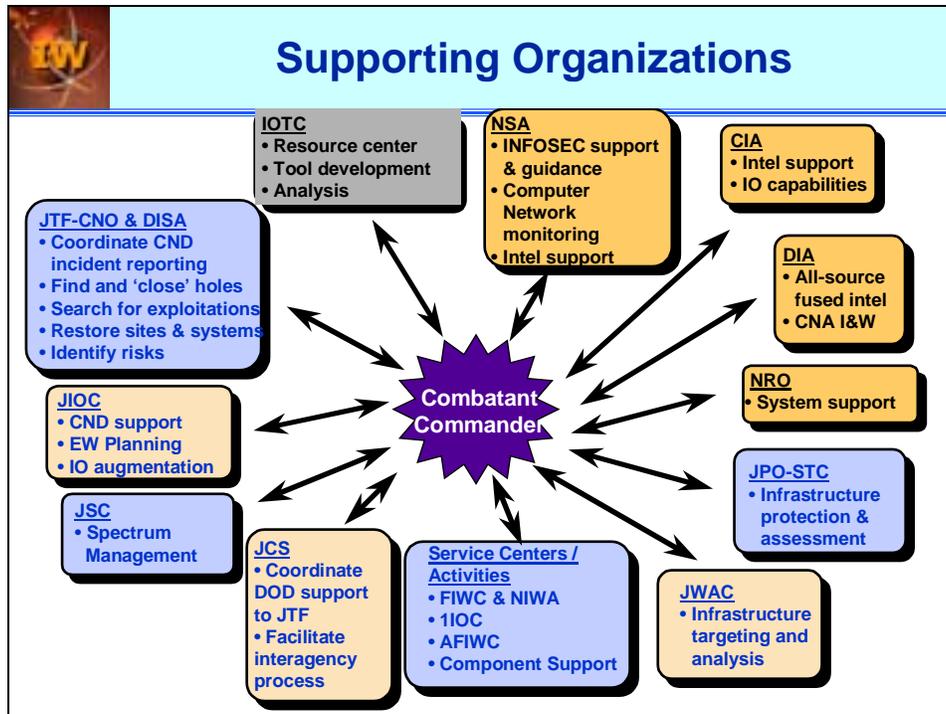
The table is from JP 3-13 Figure V-3, page V-7.

4.a(1) The following discussion of IO planning provides enhanced detail of the general guide to IO planning found in JP 3-13. As stated in JP 3-13, "The figure may be adapted for similar IO planning guidance at the subordinate joint force and component levels as required. When IO planning is being conducted below the combatant command level, the IO cell should keep the IO cell at the next higher level of command fully apprised of all IO deliberate planning activities which may require synchronization, coordination, or deconfliction."

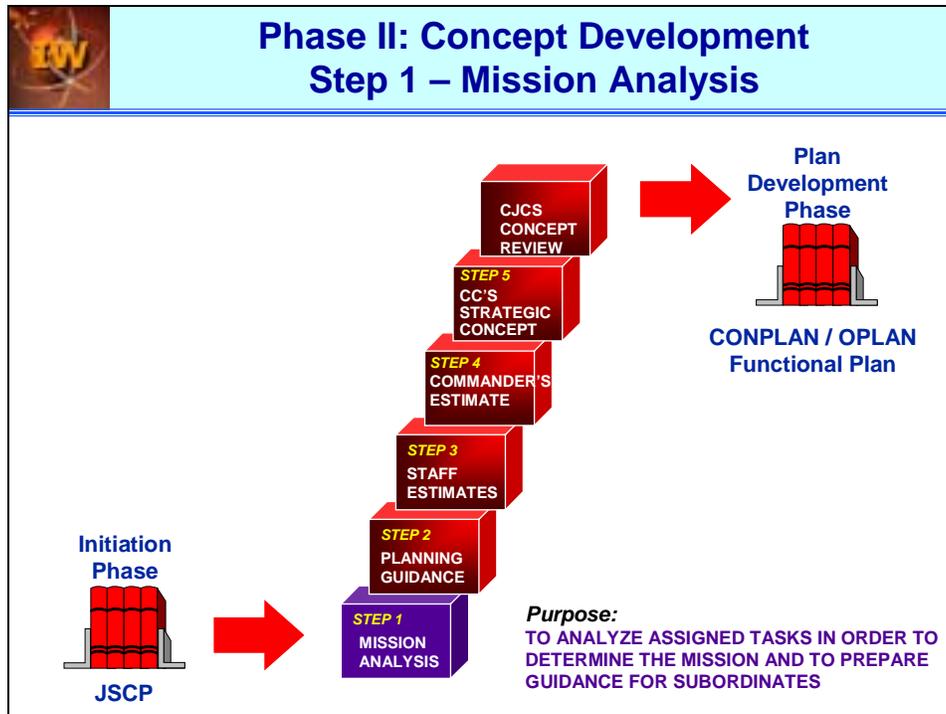




4.a(2) To begin the planning process, notify the IO cell of a planning requirement and assemble the members. Consider special augmentation for the cell, such as representatives from the JIOC, JWAC or service component IO planning staffs. Be imaginative. For example, if the Area of Operations is in an Islamic country, consider bringing a Chaplain into the planning to provide guidance on cultural and religious considerations. If the mission is disaster relief, a Surgeon may be desirable on the planning team. See Chapter II of this Handbook for a discussion of organizing an IO cell. Once the cell is assembled, the staff estimate process begins. The staff estimate process is discussed in Chapter III of this Handbook.



Do not work your planning in a vacuum. There are many planning organizations that will help you if you ask. Some of them are listed here, but this is certainly not an exhaustive list.



4.b. Phase II of the Deliberate Planning process is the Concept Development Phase. This phase consists of six steps, which are discussed individually.

4.b(1) Step 1 of the Concept Development phase is Mission Analysis. The purpose of this step is to analyze assigned tasks in order to determine the mission and to prepare guidance for subordinate elements.

	<h2>Scenario</h2>
<ul style="list-style-type: none">• Typhoons inundate Mandura• Thousands homeless• Hundreds feared dead• Embattled Manduran government requests U.S. assistance• Local insurgents threaten increased violence and kidnappings if U.S. presence in country increases	
	<h2>Mission Statement</h2>
<p>When directed, the JTF will deploy to Mandura to support force protection measures in the AOR and help deter aggression against U.S. military forces and support disaster relief operations in support of U.S. and host nation government and non-governmental organizations (NGOs).</p>	

This sample mission statement will be used to illustrate the deliberate planning process.



Mission Analysis

- **Combatant Commander reviews JCS guidelines**
 - **Specified and implied tasks**
 - **Assumptions, constraints, and restraints**
- **Analyzes**
 - **Friendly forces**
 - **Terrain and weather**
 - **Adversary**
 - **Forces and capabilities**
 - **IO systems**
- **Develop PIRs and RFIs**
- **Determine restated mission and Combatant Commander's objectives**
- **The JIOPP begins here**

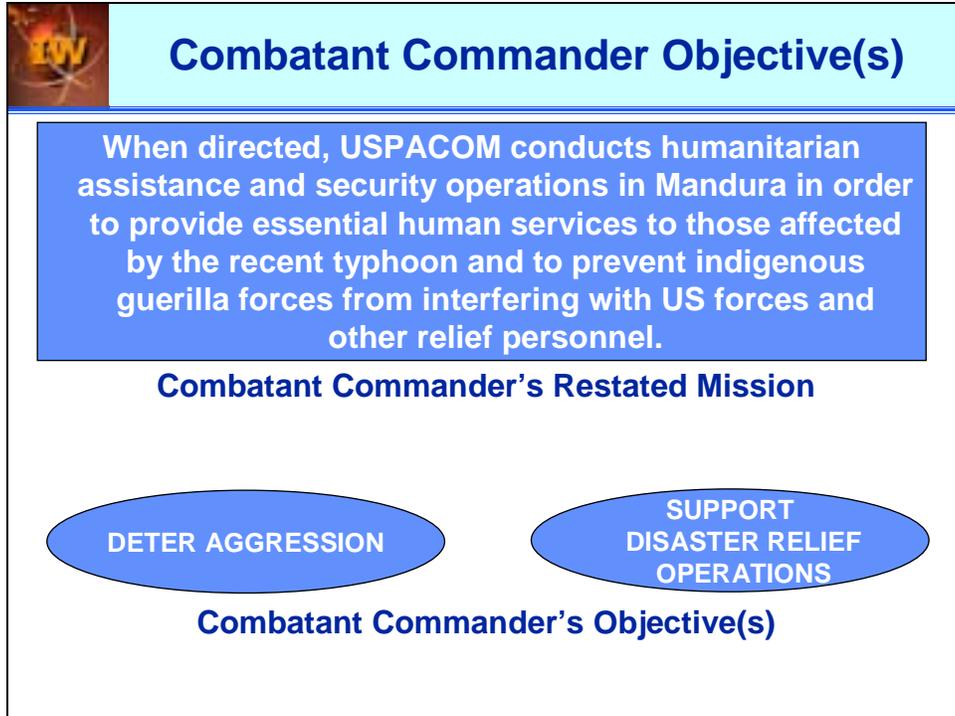
4.b(1)(a) First, a review of any JCS guidelines provided in the JSCP is conducted. Then specified tasks from the SECDEF mission are identified. Finally, any implied tasks not specifically, stated but which must be completed to accomplish the mission, are identified. Assumptions are made only if it is impossible to continue planning without them. Assumptions are always kept to a minimum. Constraints deal with factual limitations, such as a time limit placed on an operation or a supply limitation, (for example, "This operation will not exceed 30 days" or "There is sufficient POL only for 15 days of operations."). Restraints are limitations that have been imposed by the planning directive, such as ROE or specific limiting instructions (for example, "Do not violate adversary airspace.")

Analyze the friendly forces apportioned for the mission (done by the J3), the terrain and impact of weather on military operations (done by the J2), the enemy/adversary forces and capabilities (done by the J2) and enemy/adversary IO systems (done by the J2, with support by the IO cell).

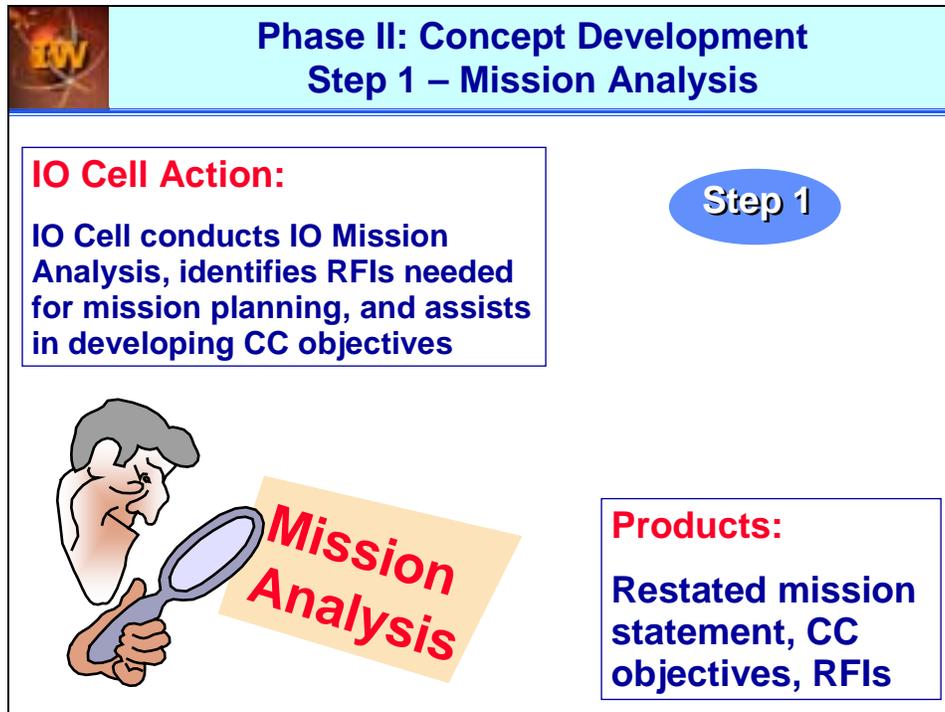
During the course of the analysis, the IO cell should develop any proposed Priority Intelligence Requirements (PIRs) specifically supporting the IO mission and develop Requests for Information (RFIs) to fill any intelligence gaps.

The final step of Mission Analysis is to determine a restated mission and the proposed CC mission objectives for the CC's approval. The next page shows the restated mission and proposed mission objectives taken from our example mission statement.

The Joint IO Planning Process (JIOPP) that is discussed in Chapters V and VI begins here and runs in parallel with the JOPES planning process.



4.b(1)(b) The restated mission will be used as the mission statement for developing the plan. The CC's objectives will be used to focus planning, using a methodology known as "Strategy-to-Task" (also sometimes called "Objective-to-Task"). The CC's objectives generally answer the question "what" the CC desires to accomplish, while the strategy answers the "how" the objectives will be accomplished.



The graphic is a rectangular box with a light blue header and a white body. The header contains the text "Phase II: Concept Development Step 1 – Mission Analysis" in blue. In the top left corner of the header is a small square icon with the letters "IIV" in yellow. The body of the graphic contains several elements: a red-bordered box on the left with the heading "IO Cell Action:" in red and the text "IO Cell conducts IO Mission Analysis, identifies RFIs needed for mission planning, and assists in developing CC objectives" in blue; a blue oval on the right with the text "Step 1" in white; a cartoon illustration of a man with a magnifying glass over a yellow sign that says "Mission Analysis" in red; and a blue-bordered box on the right with the heading "Products:" in red and the text "Restated mission statement, CC objectives, RFIs" in blue.

Phase II: Concept Development
Step 1 – Mission Analysis

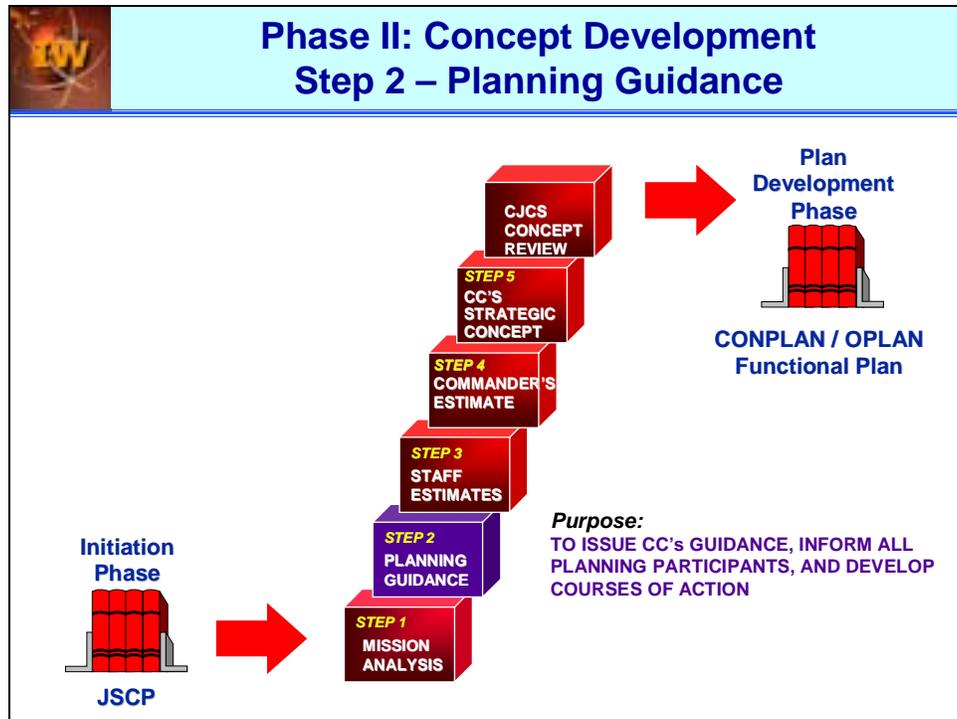
IO Cell Action:
IO Cell conducts IO Mission Analysis, identifies RFIs needed for mission planning, and assists in developing CC objectives

Step 1

Mission Analysis

Products:
Restated mission statement, CC objectives, RFIs

In review, we have just discussed Mission Analysis, which is the first step in the Concept Development phase. The graphic summarizes the preceding discussion.



4.b(2) Step 2 of the Concept Development phase is the formulation and dissemination of the CC's planning guidance to the staff. The purpose of this step is to inform all participants of the restated mission and CC's objective(s), to issue any specific planning guidance from the CC, and to develop possible courses of action for accomplishing the mission. The staff will normally develop a minimum of three proposed courses of action. The CC may specify one or more courses of action that he wants the staff to develop. The following pages discuss Planning Guidance.



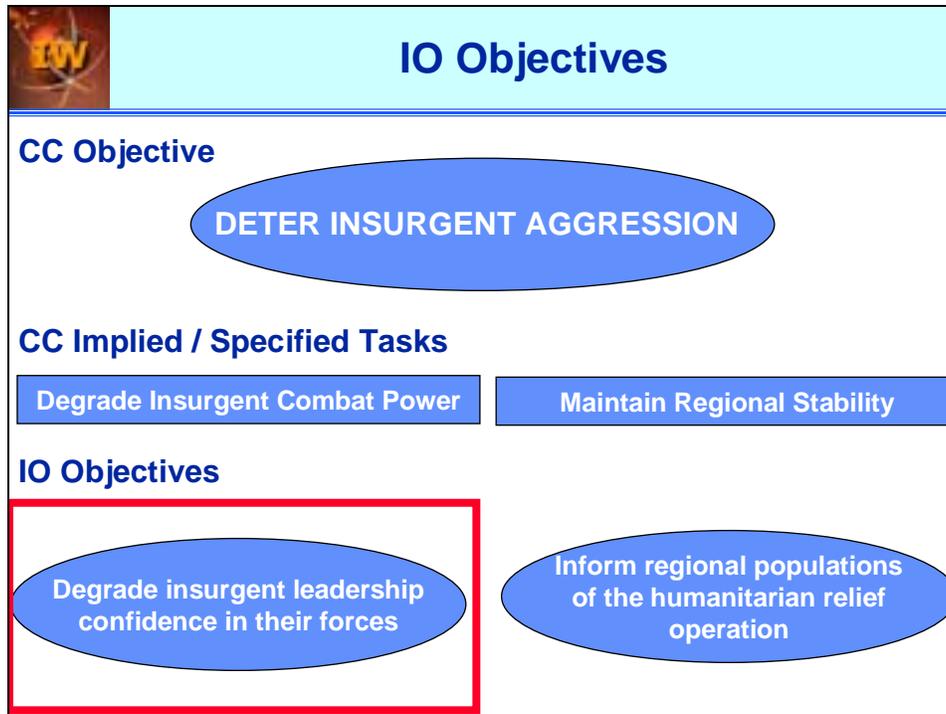
Planning Guidance

- **Consider Offensive vs. Defensive IO**
 - **Particular emphasis?**
 - **Desired effects?**
- **Ensure Commander's intent and COAs include IO issues**
- **Develop IO Objectives and Sub-objectives**
- **Develop CC's informational themes**

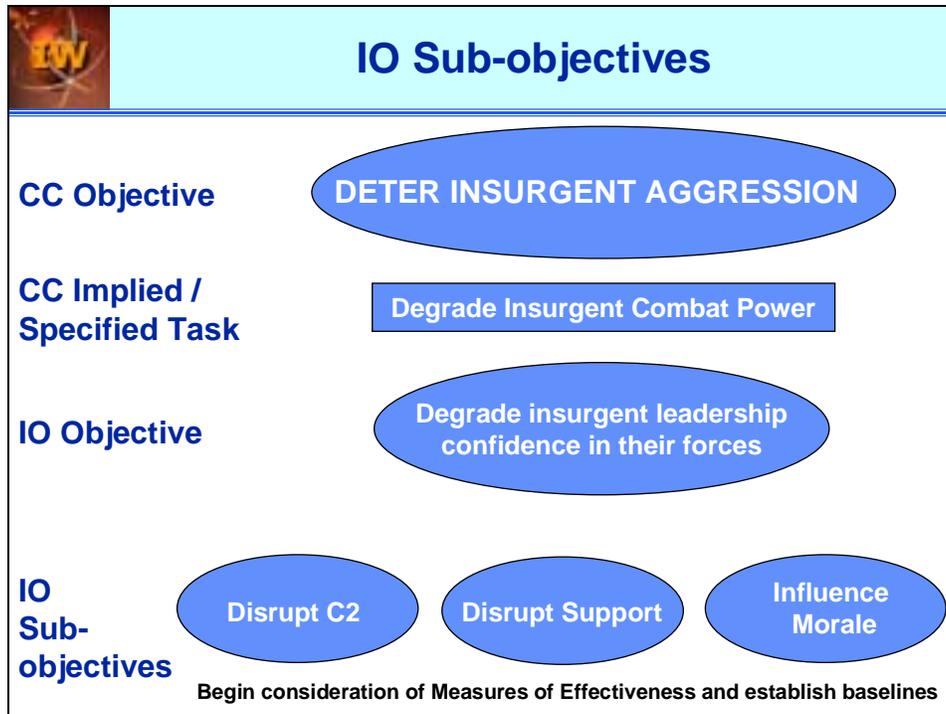
4.b(2)(a) The CC's planning guidance is normally developed by the staff and submitted to the CC for approval. He may accept the proposed guidance as is, modify it, or reject it completely and provide other guidance. The CC's planning guidance should consider both offensive and defensive IO. The CC may desire to place particular emphasis on one or the other. Ideally, the planning guidance for IO will be stated using the possible effects of IO, for example, "deny, disrupt, degrade, destroy, influence, exploit," etc.

The IO Cell chief should strive to ensure that the Commander's stated intent and all developed courses of action include IO issues.

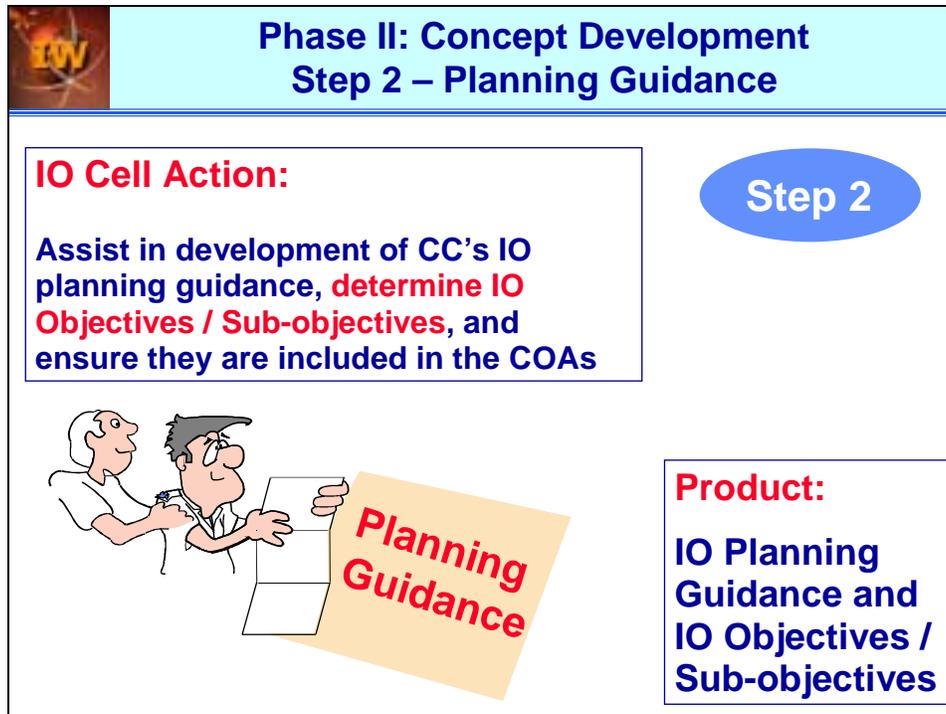
During the development of planning guidance, the IO cell will develop proposed IO objectives and sub-objectives, using the "Strategy-to-Task" methodology. The next page shows an example of this, using one of the sample CC objectives developed earlier.



4.b(2)(b) Using the CC Objective of “Deter Insurgent Aggression” which was developed earlier, two supporting IO Objectives have been developed and are shown here. On the following page, we take the IO Objective shown in the box and break it further down into IO Sub-objectives, using the “Strategy-to-Task” methodology.



4.b(2)(c) In this example, the IO Objective developed in the previous step was broken it down into three IO Sub-objectives, using the “Strategy-to-Task” methodology. At this point, the planners need to begin consideration of what measures of effectiveness they want to apply when determining if the CC IO Objectives and Sub-objectives have been achieved. The following page summarizes the steps the IO cell takes in developing the CC’s Planning Guidance.



The graphic is a rectangular box with a light blue header and a white body. The header contains the text "Phase II: Concept Development Step 2 – Planning Guidance" in blue. In the top left corner of the header is a small square icon with the letters "IIV" in orange and yellow. The body of the box contains three main elements: a red-bordered box on the left with the text "IO Cell Action:" followed by "Assist in development of CC's IO planning guidance, determine IO Objectives / Sub-objectives, and ensure they are included in the COAs"; a blue oval on the right containing the text "Step 2"; and a white-bordered box on the right containing the text "Product:" followed by "IO Planning Guidance and IO Objectives / Sub-objectives". At the bottom left of the body is a cartoon illustration of two men in white shirts looking at a large yellow document that says "Planning Guidance" in red.

Phase II: Concept Development
Step 2 – Planning Guidance

IO Cell Action:

Assist in development of CC's IO planning guidance, **determine IO Objectives / Sub-objectives**, and ensure they are included in the COAs

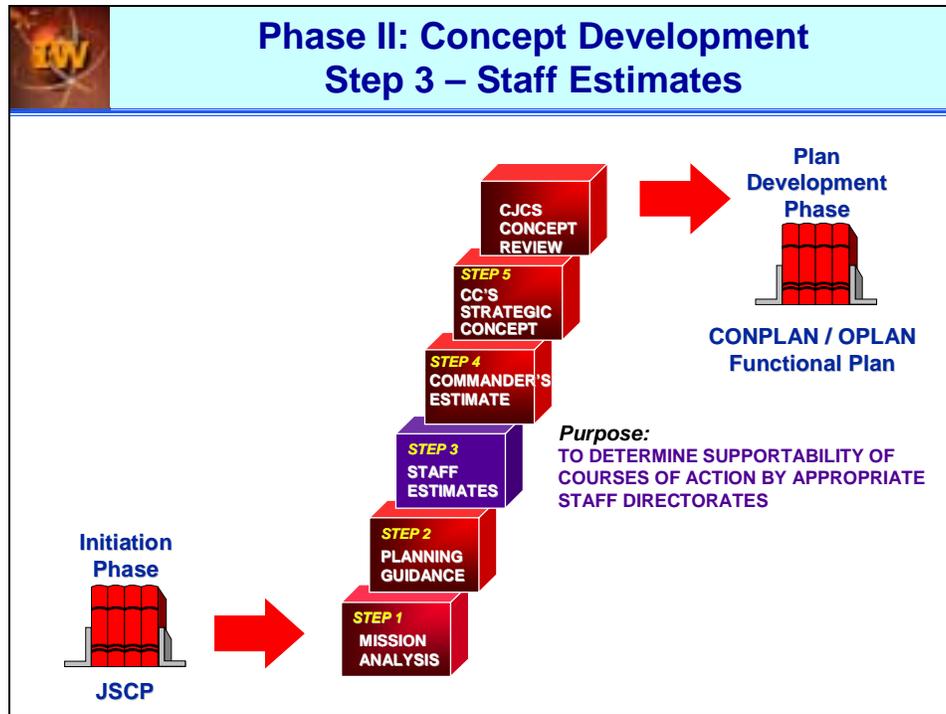
Step 2

Product:

IO Planning Guidance and IO Objectives / Sub-objectives



This completes the discussion of Planning Guidance, which is Step 2 in the Concept Development phase. Now on to Step 3, the Staff Estimates of Supportability.



4.b(3) Step 3 of the Concept Development phase is conducting Staff Estimates of Supportability. In this step, each staff element, including the IO cell, compares and contrasts each proposed course of action in order to prioritize the courses of action in the order of supportability from most supportable to least supportable. Depending upon the desires of the J3, the IO Cell may develop its own staff estimate of supportability or it may contribute to the J3 estimate. The following pages describe the actions that all staff elements must take during the estimate process.



Staff Estimates of Supportability

- **Each staff element, including the IO Cell, must:**
 - **Review the mission and situation from its own narrow functional perspective**
 - **Examine the factors for which it is the responsible staff**
 - **Analyze each COA from its staff functional perspective**
 - **Compare each COA based on its staff functional analysis**
 - **Conclude whether the mission can be supported and which COA can best be supported from its particular staff functional perspective**

4.b(3)(a) This describes some basic considerations for conducting a Staff Estimate of Supportability. Regardless of whether the IO Cell develops its own estimate or contributes to the J3 estimate, consideration must be given to whether each course of action is supportable from the IO perspective. It is important that the IO Cell participate in the development of the Intelligence and Communication staff estimates, as these functions will provide support to Information Operations. The following page gives a summary.



Phase II: Concept Development Step 3 – Staff Estimates

IO Cell Action:

Develop IO estimate of supportability and assist in the development of intelligence, operations, and communications staff estimates

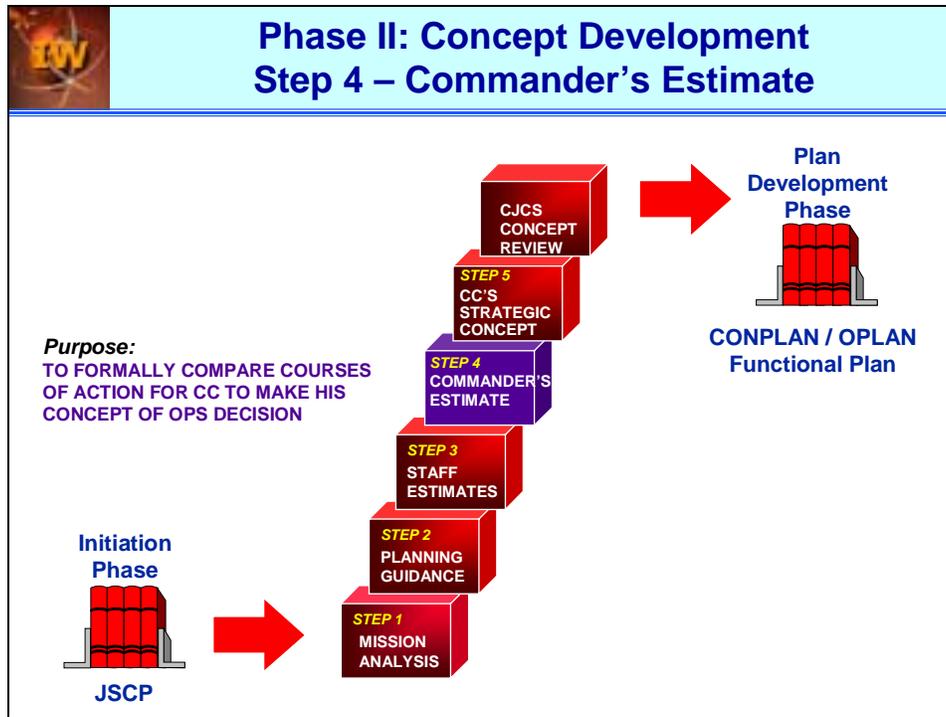
Step 3



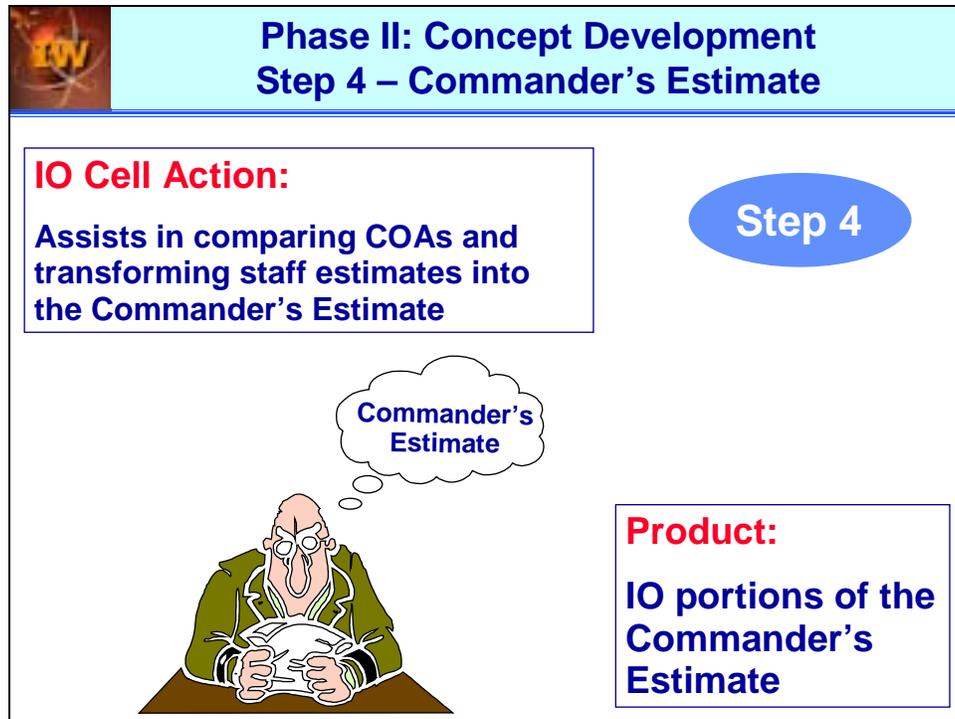
Products:

IO staff estimate (if required) and IO portions of other staff estimates

This completes the discussion of developing the Staff Estimates of Supportability, which is Step 3 in the Concept Development phase. Now on to Step 4, the Commander's Estimate.



4.b(4) Step 4 of the Concept Development Phase is the Commander's Estimate. The purpose of this step is to formally compare the proposed courses of actions by means of a decision briefing to the CC. At the end of the decision briefing, the CC is asked to select a course of action for which the staff will proceed to develop the plan. The CC may select one of the proposed courses of action as is, select a course of action with modifications, or choose an entirely different course of action.



Phase II: Concept Development
Step 4 – Commander's Estimate

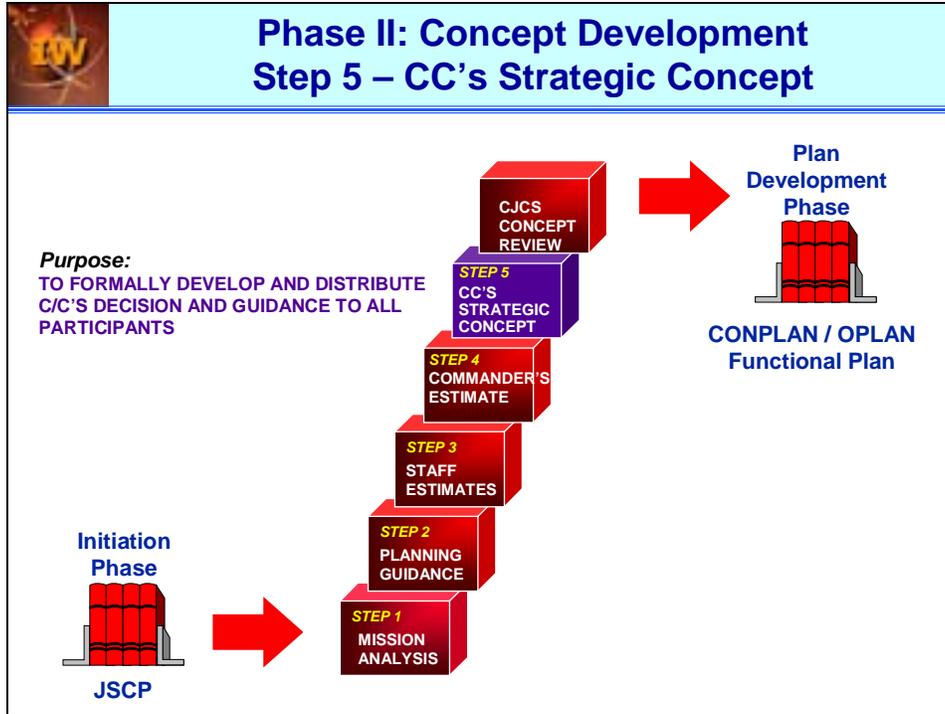
IO Cell Action:
Assists in comparing COAs and transforming staff estimates into the Commander's Estimate

Step 4

Product:
IO portions of the Commander's Estimate

Commander's Estimate

The IO Cell will assist in comparing courses of action and transforming staff estimates into the Commander's Estimate. If the IO Cell is required to prepare a separate Staff Estimate of Supportability, the Cell will normally brief (or have briefed) its estimate to the CC as part of the overall decision briefing. The Commander's Estimate process is complete when the CC selects a course of action.



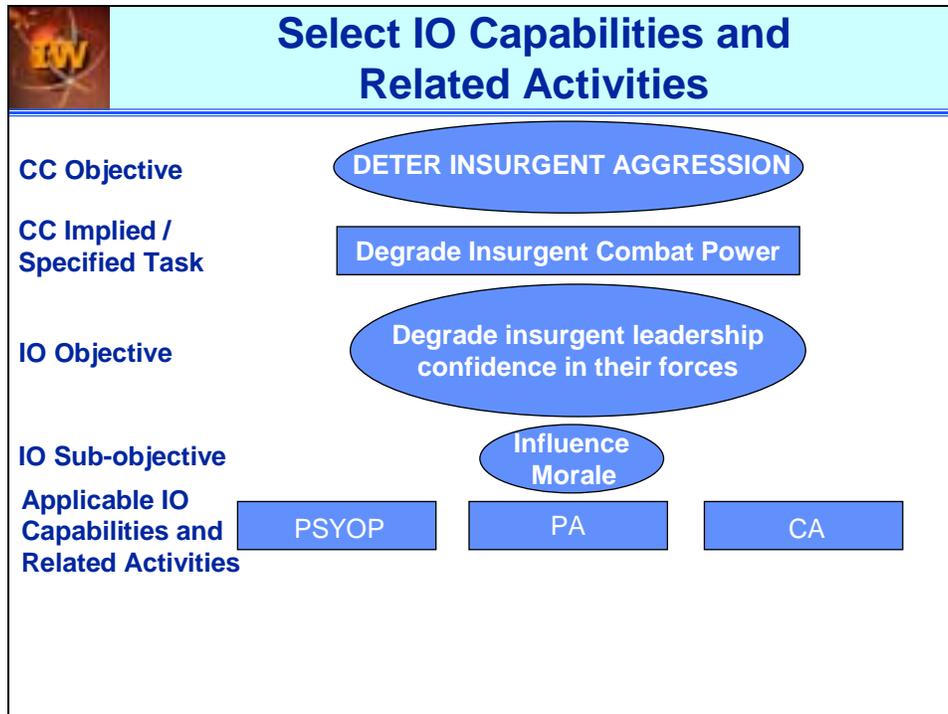
4.b(5) Step 5 of the Concept Development Phase is Developing the CC's Strategic Concept. The purpose of this step is to formally develop and distribute the CC's course of action selection and further guidance to all participants in the planning process. Amongst the guidance disseminated with the CC's Strategic Concept should be IO themes to be used in support of Public Affairs, Civil Military Operations, and PSYOP for each phase of the operation. The themes for each of these areas should be totally complementary so as to avoid sending mixed messages that might cause an adversary to respond in a manner that was not anticipated.



Phase II: Concept Development Step 5A – CC's Strategic Concept

A. Select IO capabilities and related activities

4.b(5)(a) With a course of action selected, it's now time to begin adding some detail to the planning. To do this, the IO Cell continues using the "Strategy-to-Task" methodology and selects specific IO capabilities and related activities to support the IO Sub-objectives developed previously.



4.b(5)(b) To accomplish the IO Sub-objective “Degrade Morale,” the IO Cell has elected to employ the capabilities of psychological operations, public affairs, and civil affairs. Other capabilities and related activities could have been chosen as well, depending upon the capabilities and forces available to the command.



Phase II: Concept Development Step 5B – CC's Strategic Concept

- A. Select IO capabilities and related activities
- B. Determine priority of IO effort**

4.b(5)(c) Having selected the applicable IO capabilities and related activities, the IO Cell must determine the priority of effort for each capability or related activity. The priority of effort may change for each phase of an operation. The next page shows an example of a priority of effort matrix that may serve as a useful tool in visually depicting the IO priorities for each IO capability and related activity.

Priority of Effort Matrix							
CC Objective	Deter Insurgent Aggression						
IO Objective	Degrade Insurgent Leadership Confidence in Their Forces						
IO Sub-objective	CA	PA	OPSEC	PSYOP	DECP	EW	DEST
Disrupt C2		S	S	S	P2	P1	
Disrupt Support			S	S	P2	P1	
Reduce Morale and Loyalty		S	S	P1	P2	S	
Exploit C2				S	P2	P1	
Publicize poor Insurgent tech vs. US		P2	S	P1	S	S	
Publicize lack of internal support	S	P1		P2			
Reduce confidence in intel			S	P2	P1	S	
Publicize lack of external support		P1		P2		S	

4.b(5)(d) Using the “Strategy-to-Task” methodology, this example reduces the CC Objective “Deter Insurgent Aggression” to an IO Objective and associated IO Sub-objectives.

The matrix shows which capability or related activity will have primacy in supporting each IO Sub-objective. “P1” indicates the primary effort. “P2” represents the secondary effort. “S” indicates a supporting effort. A blank space indicates that a given capability or related activity is not tasked in the effort to accomplish the specific IO Sub-objective.

(Note: Computer Network Attack was intentionally omitted from this example.)



Phase II: Concept Development Step 5C – CC's Strategic Concept

- A. Select IO capabilities and related activities
- B. Determine priority of IO effort
- C. Consider coordination or conflict**

4.b(5)(e) Having established the priority of effort for IO capabilities and related activities, the IO Cell must now consider coordination and potential conflict between the capabilities and related activities.

Deconflicting IO	
Example of what could go wrong	
<i>Destruction</i>	ATO / ITO is published and all SIGINT sites are targeted
<i>EW</i>	COMPASS CALL tasked to jam frequencies from 61.95 MHz to 92.45 MHz
<i>Psychological Operations</i>	COMMANDO SOLO tasked to transmit messages on 62.35 MHz. Uncoordinated leaflet drop to the front of the notional Corps Hqs that supports the deception plan.
<i>Military Deception</i>	Notional Corps Hqs broadcasting on frequencies 62.00 MHz to 69.95 MHz
<i>OPSEC</i>	Discussion of integration problems over unsecured lines could lead to the compromise of the overall plan
<i>PA</i>	PA release discloses presence of COMMANDO SOLO
<i>CA</i>	CA developing civilian emergency communication net to transmit over 63 MHz

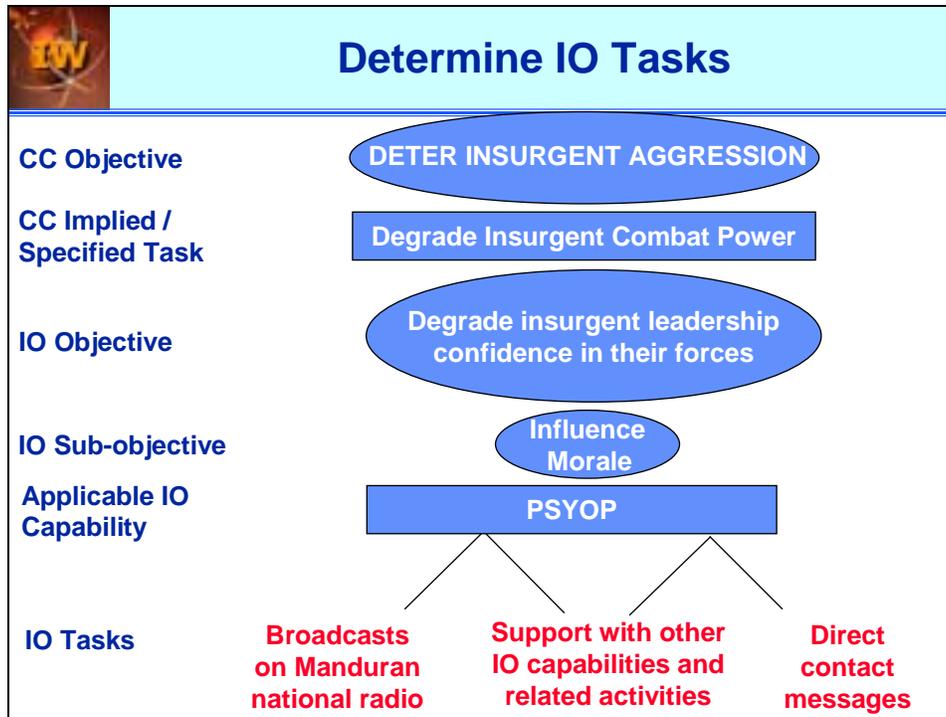
4.b(5)(f) Capabilities and related activities can be mutually supportive or be directly opposed to one another. Gain/loss must be considered when doing deconfliction. (Note: Computer Network Attack was deliberately omitted from this example.)



Phase II: Concept Development Step 5D – CC's Strategic Concept

- A. Select IO capabilities and related activities
- B. Determine priority of IO effort
- C. Consider coordination or conflict
- D. Determine IO tasks**

4.b(5)(g) Having conducted coordination and deconfliction of the IO capabilities and related activities, the IO Cell should now determine specific tasks for each capability and related activity.



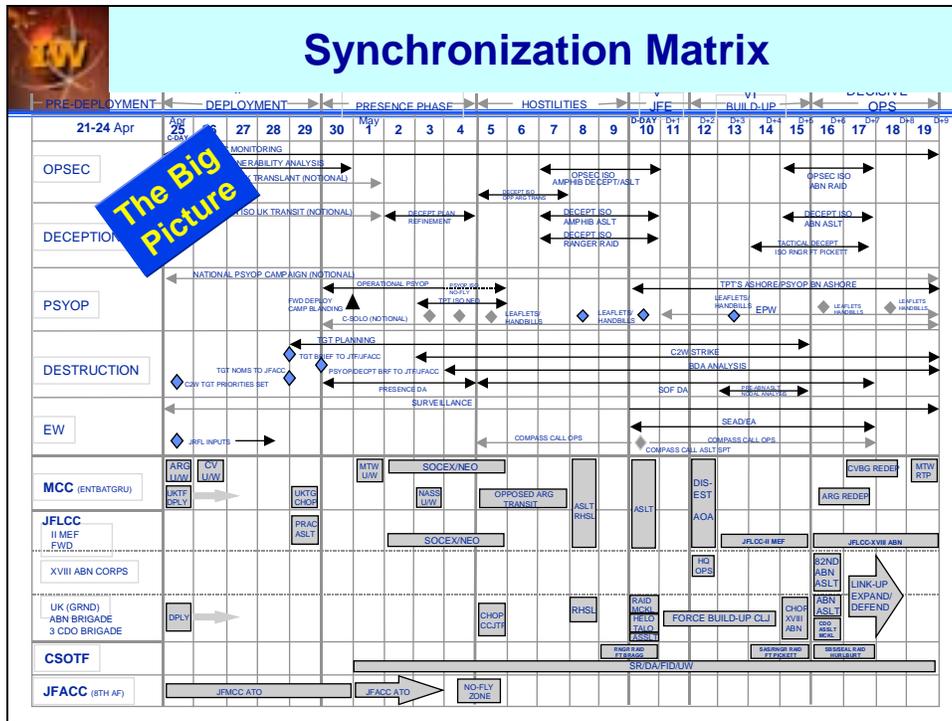
Choose tasks that are appropriate for the chosen IO capability.



Phase II: Concept Development Step 5E – CC's Strategic Concept

- A. Select IO capabilities and related activities
- B. Determine priority of IO effort
- C. Consider coordination or conflict
- D. Determine IO tasks
- E. Synchronize IO capabilities**

4.b(5)(h) Once the IO tasks have been determined, it is time for the IO cell to begin the last step in helping develop the Commander's strategic concept. This step involves synchronizing the IO capabilities and related activities to achieve a synergy from their combined effects.



This example, taken from a Joint Task Force Exercise, shows how a synchronization matrix might be used. Entered across the top are the phases of the operation that are broken down into days. Down the left side are the IO capabilities and related activities and the major forces apportioned to support the OPLAN.

This sample matrix is completed to indicate the activities of the major forces at any given time during the operation in the bottom portion. The upper portion includes the actions of the IO capabilities and related activities that will support the operation. This simple use of a synchronization matrix will help ensure that the necessary IO support is planned for and available during the execution of the plan.



Phase II: Concept Development Step 5 – CC's Strategic Concept

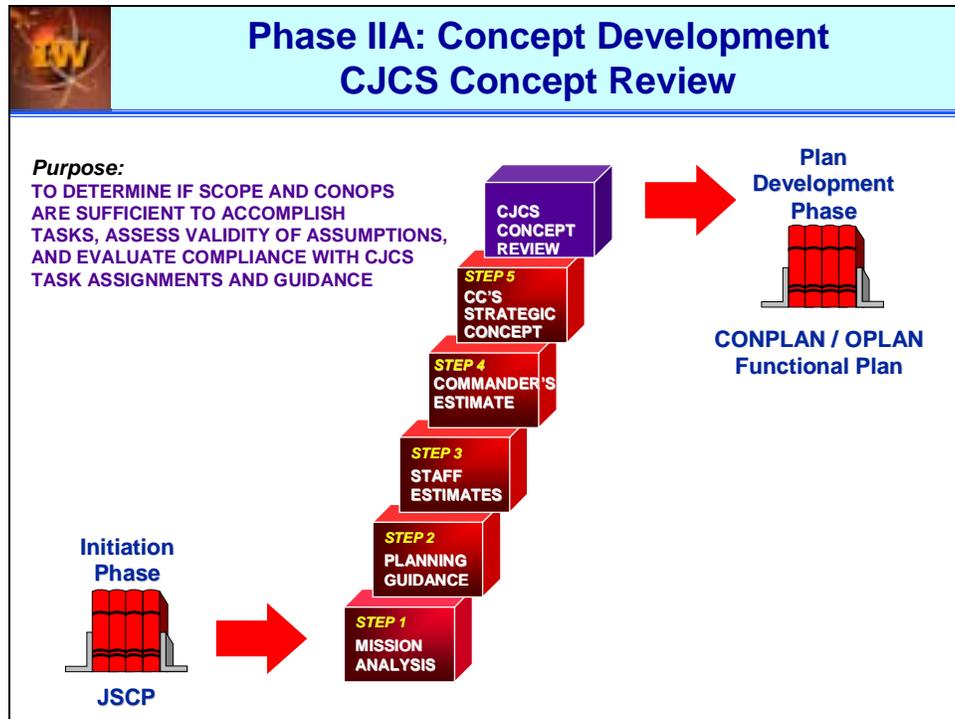
IO Cell Action:
Assist in developing the selected COA into a CONOPs, and determine applicable IO capabilities / related activities and tasks

Step 5



Product:
Select IO Capabilities, Priority of Effort Matrix, Synchronization Matrix and IO portion of CC's Strategic Concept

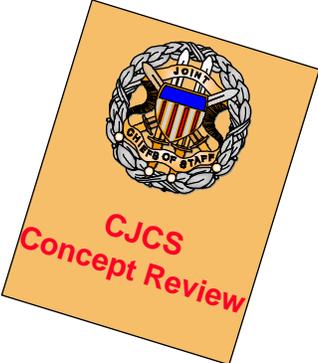
This is a summary of the development of the CC's Strategic Concept.



4.b(6) Step 6 of the Concept Development phase is developing the CJCS Concept Review. The purpose of this step is to formally examine the submitted plan for completeness and to ensure that unapproved objectives or tasks are not included.

Phase IIA: CJCS Concept Review

IO Cell Action:
Continue planning
selected COA



Product:
None

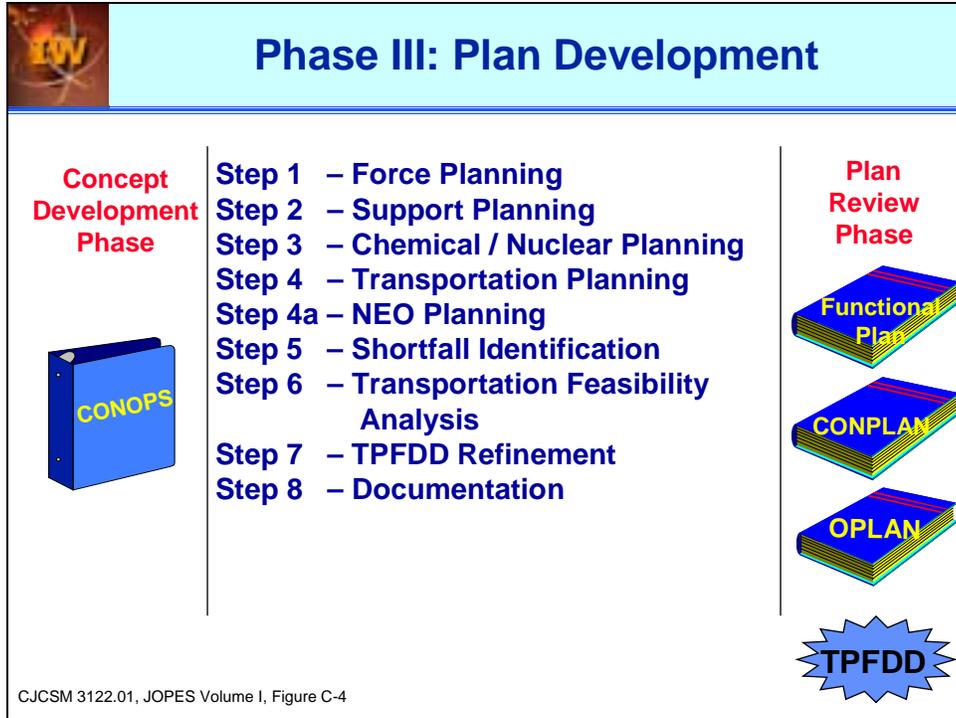
The diagram is a rectangular box with a light blue header containing the text "Phase IIA: CJCS Concept Review". Below the header, on the left, is a white box with a blue border containing the text "IO Cell Action: Continue planning selected COA". In the center is a tilted orange rectangle containing the CJCS seal and the text "CJCS Concept Review". On the right is a white box with a blue border containing the text "Product: None".

This step involves a “wait and see” period for the CJCS Concept Review. Of course, a good IO Cell will be continue to plan based upon the assumption that the CJCS review of the CC’s Strategic Concept will be favorable. Next comes Phase III of the Deliberate Planning Process, the Plan Development Phase.

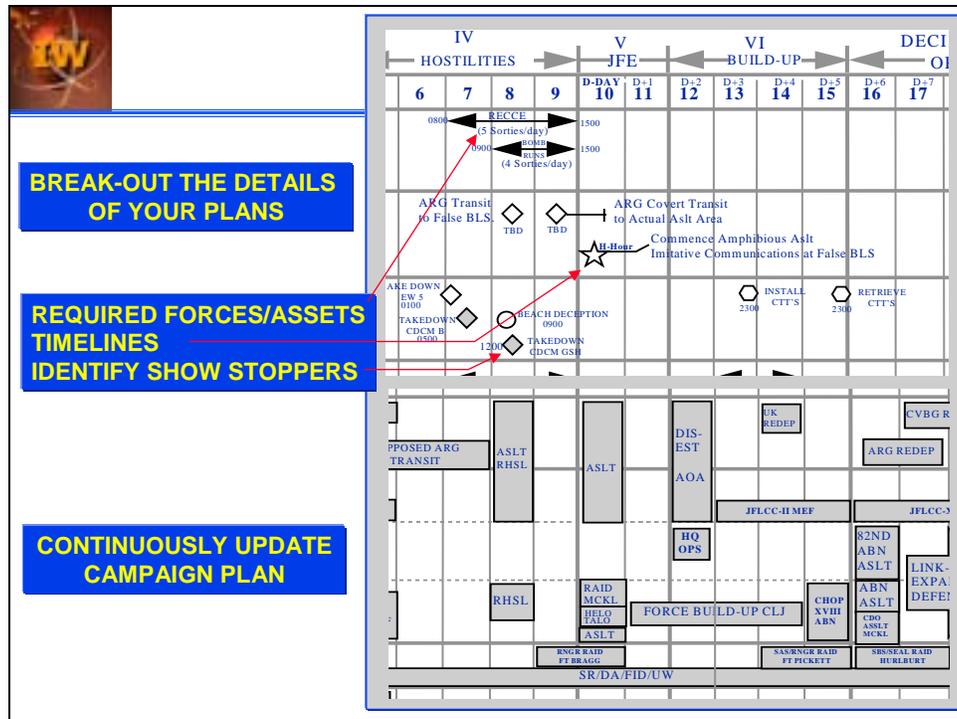


Concept Review Results

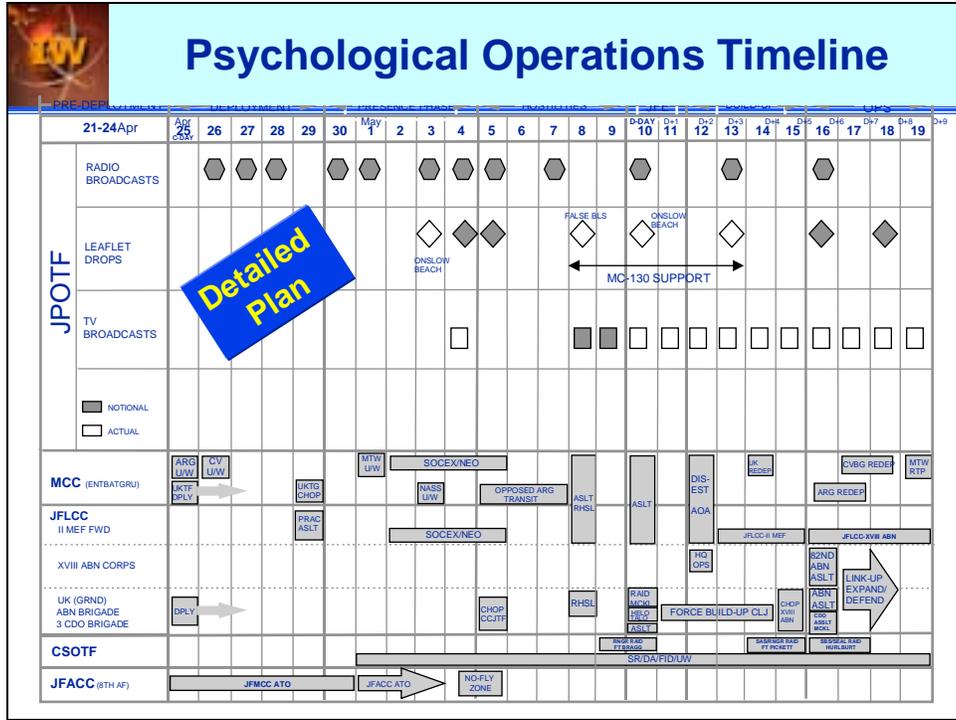
- **Approved** - Goes back to Combatant Commander for further plan development
- **Disapproved** - Requires significant change prior to re-submission and must be corrected within 30 days



4.c. Phase III of the Deliberate Planning process is the Plan Development Phase. During this phase, all staff elements, including the IO Cell, begin to work the fine details of their particular aspect of the plan and coordinate this with other applicable staff elements. The IO Cell must pay particular attention to coordination with the Intelligence, Communications, and Legal staff elements, without overlooking any of the IO capabilities or related activities.



4.c(1) This example, also from a Joint Task Force Exercise, shows some areas of particular concern. The IO Cell must develop specific details of the IO plan, to include required forces/assets, timelines, and any showstoppers that must be paid particular attention. For example, failure to effectively shut down a particular air defense missile site may be a showstopper that could affect the command's ability to accomplish the mission if not reconciled. The IO Cell must remain keenly aware of changes in the OPLAN that will require changes in the IO planning.



4.c(2) A sample JTFEX synchronization matrix for a PSYOP operation is presented. During the Concept Development Phase, a single synchronization matrix depicted all of the IO capabilities and related activities. During the Plan Development Phase, the detailed planning will necessitate developing a separate synchronization matrix for each IO capability and related activity. Only PSYOP is shown in the example.



IO Planning Worksheet

IO PLANNING WORKSHEET - BOSNIACS			
TARGET GROUP	VITAL INTERESTS	ACTION, THEMES, & MEDIUMS TO ACHIEVE VITAL INTEREST	PRESSURE POINTS
National Politicians	Regain territory lost during the war	Conduct an aggressive DPRE campaign	Influence refugee flow (number, timing & location)
		Use the ballot box to win political control over selected areas	Expose political corruption Monitor Elections
		Influence the international community to favor the Bosniac position	Counter Bosniac propaganda & disinformation
	Render the IEBL politically untenable as a border	Use right of return and freedom of movement to dispel the notion the IEBL is an international border	Control movement across the Zone of Separation (ZOS)

One sure way to get the target's attention is influence something that is linked to one of their vital interests!

A "Pressure Point" is an important, essential, or primary factor that can be influenced to control behavior.



4.c(3) In order to develop the degree of detail necessary during the Plan Development Phase, it is necessary to use some information management tools.

The 1st Information Operations Command (Land) [formerly LIWA] at Fort Belvoir, VA developed the technique shown in the graphic for use in Bosnia. This and the following worksheet show examples of a consolidated IO worksheet. You should note that supporting worksheets showing the details for each capability and related activity are also necessary. In this particular example, the National Politicians of the ethnic groups in Bosnia are the targets. Their vital interests are shown in the second column. The third column shows methods the target group may employ to achieve their vital interests. The last column shows "pressure points" the CC may use as leverage as part of an IO plan to manage the perception of the particular target group.

The next page shows how this "pressure point" methodology is used to develop additional details for the IO plan.



Develop Details of the Execution Plan

IO Planning Worksheet Execution Matrix			
TARGET: National-Level Bosniac Politicians			
PRESSURE POINT: Influence refugee flow (number, timing, location)			
OBJECTIVE: Cause Bosniac politicians to promote resettlement in less contentious areas			
Phase I (14 Dec 96 - 1 Jan 97)	Phase II (2 - 28 Jan 97)	Phase III (29 Jan - 28 Feb 97)	Phase IV (1 Mar - 15 Apr 97)
<ol style="list-style-type: none"> 1. Radio & TV Spots 2. PAO & PSYOP 3. 14-21 Dec 96 4. Prepare radio & TV spots stressing it is irresponsible for elected officials to encourage refugees to return to certain areas 5. Place public pressure on elected officials 	<ol style="list-style-type: none"> 1. Press Releases 2. PAO 3. 5-20 Jan 97 4. Distribute information about mines & other hazards in some areas 5. Discourage resettlement in selected areas 	<ol style="list-style-type: none"> 1. Posters & Handbills 2. PSYOP 3. 29 Jan - 28 Feb 97 4. Distribute materials stressing the importance of following approved resettlement procedures 5. Slow the rate of return/resettlement 	<ol style="list-style-type: none"> 1. Civil Works 2. G5/Div. Engineer 3. 5-30 Mar 97 4. Arrange improvements to roads & bridges in selected areas 5. Encourage return/resettlement to areas favorable to friendly objectives
<ol style="list-style-type: none"> 1. Coordination with IOs 2. G5 - Civil Affairs 3. 14-31 Dec 96 4. Ask IOs to scrutinize all resettlement/return applications 5. Influence the pace of resettlement/return 	<ol style="list-style-type: none"> 1. Meetings w/Gov't Reps 2. POLAD/Cmd Group 3. 14 Jan 97 4. Meet with RS gov't officials to discuss resettlement policy 5. Stress the benefits of cooperation 	<ol style="list-style-type: none"> 1. Town Hall Meetings 2. TF Commanders 3. 12-28 Feb 97 4. Hold town hall style meetings in sector 5. Encourage populations to hold gov't officials accountable 	<ol style="list-style-type: none"> 1. Press Coverage 2. PAO/G5 3. 5-30 Mar 97 4. Publicize infrastructure improvements in selected areas 5. Encourage resettlement in selected areas
1=What; 2=Who Engages; 3=When; 4=Action; 5=Purpose			

4.c(4) In this example, the target group from the previous worksheet has been narrowed to a specific ethnic group, “Bosniac Politicians” (as opposed to Serb or Croat politicians). Specific IO activities have been planned based upon the phases of the operation. During the actual execution of the plan, the activities shown on this worksheet would be transferred to a daily execution checklist. The daily execution checklist is discussed later in this section. Although this type matrix is not the only means of managing the detailed planning necessary for IO, each IO cell must develop some means of managing its planning information. An SOP and database are essential to the operation.



Add Additional Detail to the Execution Plan

IO cell representatives complete an IO Implementation Worksheet listing details of each IO action.

IO IMPLEMENTATION WORKSHEET					
Category (See Codes)	When (Date)	Action	Target(s)	Primary Themes (See Codes)	Purpose
1	14 Dec 96	Broadcast taped commentary from the Bosniac radio station in Tuzla every 2 hours	National-level Bosniac politicians; specifically Petro Drko, Minister of Refugees	DP1 & DP5	Use public opinion to pressure Bosniac officials to comply with the Dayton Peace Accord (DPA)
2	30 Jan 97	Distribute handbills in Tuzla, Garli & Tranbil	Bosniac mayors of Tuzla, Garli & Tranbil	DP2 & DP4	Encourage targets not to support Violent demonstrations

The IO Implementation Worksheet is used by members of the IO Cell to provide specific details on how they will implement the action reflected on the Synchronization Matrix

CATEGORY CODES

1. PSYOP RADIO MESSAGE (COMMENTARY)	10. CIVIL AFFAIRS
2. PSYOP RADIO MESSAGE (THEMATIC BURST)	11. JMC MEETING
3. PSYOP HANDBILL	12. JMC BILAT
4. PSYOP LOUDSPEAKER	13. 2D BRIGADE
5. PRESS CONFERENCE	14. TF 1/18
6. PRESS RELEASE	15. TF 1/26
7. PRESS GUIDANCE	16. IPTF
8. PUBLIC AFFAIRS RADIO SPOT	17. COMMAND GROUP
9. POLAD MEETING	

APPROVED THEMES

MESSAGES FOR PUBLIC OFFICIALS

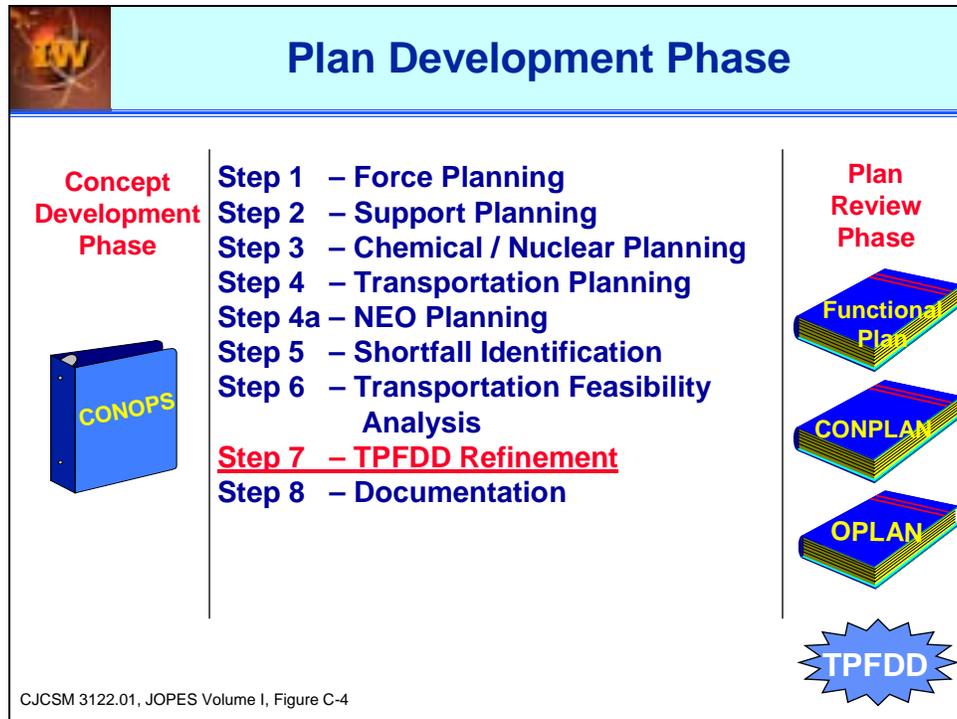
MESSAGES FOR MILITARY LEADERS

MESSAGES FOR POLICE & SPECIAL POLICE

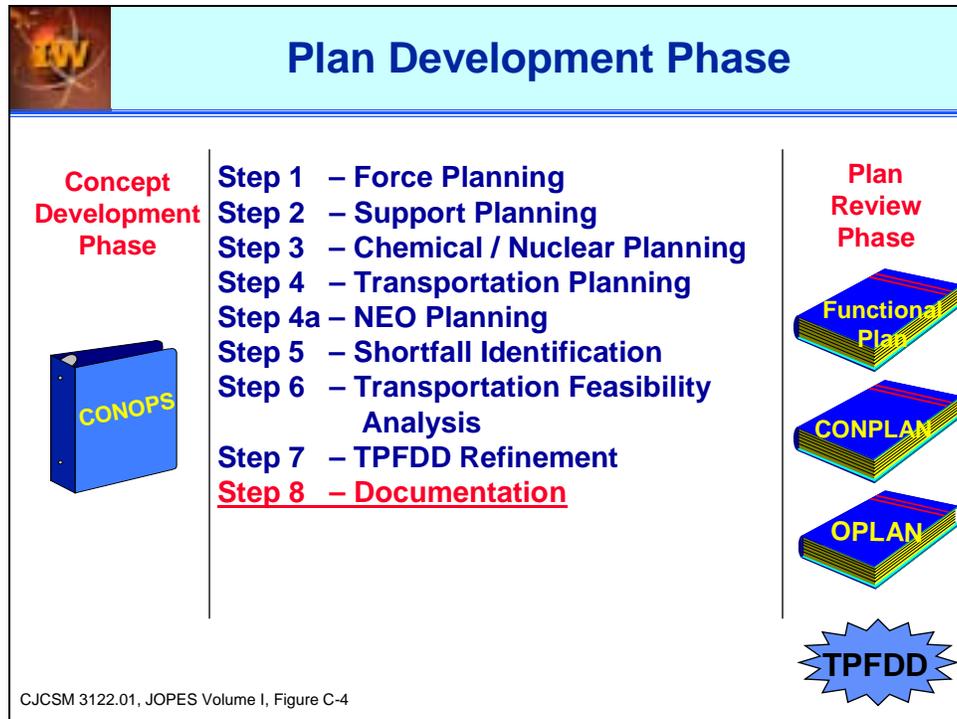
MESSAGES FOR THE GENERAL PUBLIC

As you see, the example identifies a specific date, target, and info themes

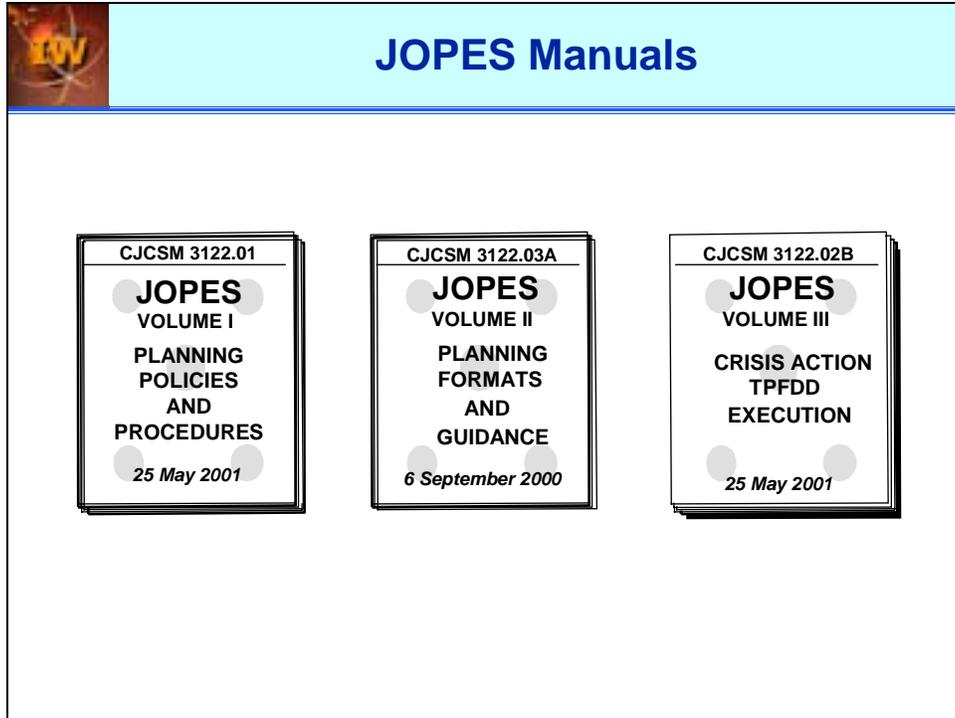
4.c(5) Continuing from the previous example, the IO Implementation Worksheet above adds yet another level of detail to the IO Planning Worksheet. In this case, specific IO tasks are identified for execution at a specific date and time. The planners have not only identified the task, but the target, specific themes, and the purpose behind the task. These details will be transferred to a daily IO execution checklist.



4.c(6) Although the refinement of the Time Phased Force Deployment Data (TPFDD) is not the responsibility of the IO Cell, it is important that the IO Cell Chief review the TPFDD to ensure that the necessary IO forces have the appropriate place in the flow of forces into the CC's area of responsibility. This is particularly important for forces that have a low density in the active component, such as PSYOP, and Civil Affairs or forces that are found only in the reserve component, such as Commando Solo. The deployment and employment of these low-density forces will require some degree of micro-management. As a rule of thumb, the CC will want to have the Civil Affairs and PSYOP units placed early in the flow of forces into theater.



4.c(7) The last step of plan development is to document everything that has been planned. This is done using the formats found in Volume II of JOPES.



4.c(8) For the purpose of IO planning, the focus will be on three volumes of JOPES.

Volume I sets forth planning policies and procedures to govern the joint activities and performance of the Armed Forces of the United States. It provides military guidance for the exercise of authority by combatant commanders and other joint force commanders and prescribes doctrine and selected joint tactics, techniques, and procedures for joint operations and training. It provides military guidance for use by the Armed Forces in preparing their appropriate plans. It discusses planning policies and procedures and addresses some aspects of IO specifically.

Volume II sets forth administrative instructions and formats to govern the development of joint operation plans submitted for review to the CJCS. It contains the basic format for an OPLAN and its related annexes and appendices.

Volume III sets forth procedures for the development of Time-Phased Force and Deployment Data (TPFDD) and for the deployment and redeployment of forces within the context of the Joint Operation Planning and Execution System (JOPES) in support of joint military operations. Military guidance for the exercise of authority by combatant commanders and other joint force commanders for joint operations and training using JOPES.

JOPES manuals may be downloaded from the limited CJCSM page accessible from <http://www.dtic.mil/doctrine/>.

 Operation Plan Annexes	
A Task Organization	L Environmental Considerations
B Intelligence	M Geospatial Information and Services
<u>C Operations</u>	N Space Operations
D Logistics	P Host-Nation Support
E Personnel	Q Medical Services
F Public Affairs	S Special Technical Operations
G Civil Affairs	T Consequence Management
H Meteorological and Oceanographic Operations	V Interagency Coordination
J Command Relationships	X Execution Checklist
K Command, Control, Communications and Computer Systems	Z Distribution

4.c(9) The majority of the IO information in the OPLAN will be located in **Annex C, Operations**.

Annex B will contain all intelligence information, to include that specifically related to IO. Annex C, Appendix 3 should direct the reader to those paragraphs in Annex B that applies specifically to IO.

Annex F will contain all public affairs information, to include that specifically related to IO. Annex C, Appendix 3 should direct the reader to those paragraphs in Annex F that applies specifically to IO.

Annex G will contain all civil affairs information, to include that specifically related to IO. Annex C, Appendix 3 should direct the reader to those paragraphs in Annex G that applies specifically to IO.

Annex K will contain all C3 information. Annex C, Appendix 3 should direct the reader to those paragraphs in Annex K that applies specifically to IO.

Annex N will contain SPACE information related to IO to include CND and CNA operations.

Annex S will contain compartmented information on computer network attack.

Annex T is a new annex that provides guidance for planning and executing consequence management operations (NBC only).

Annex V is a relatively new annex. It contains information on interagency coordination and addresses any interagency participation/action desired to execution the IO portion of the plan. The annex is not directive in nature, so close coordination is essential to ensure interagency support for the CC's IO.



Information Operations Appendix

- **Appendix 3 to Annex C**
- **Contains 6 (or 7) Tabs**
 - **Tab A - Military Deception**
 - **Tab B - Electronic Warfare**
 - **Tab C - Operations Security**
 - **Tab D - Psychological Operations**
 - **Tab E - Physical Attack / Destruction**
 - **Tab F - Computer Network Attack**
 - **Tab G - Defensive Information Operations**

4.c(10) In Annex C, you will find **Appendix 3, Information Operations** (formerly called the C2W Appendix), containing the following tabs:

Tab A – Military Deception

Tab B – Electronic Warfare (EW)

Tab C – Operational Security (OPSEC)

Tab D – Psychological Operations (PSYOP)

Tab E – Physical Destruction

Tab F – Computer Network Attack (may also be in Annex S (STO))

Tab G – Defensive Information Operations



Phase III: Plan Development

IO Cell Action:

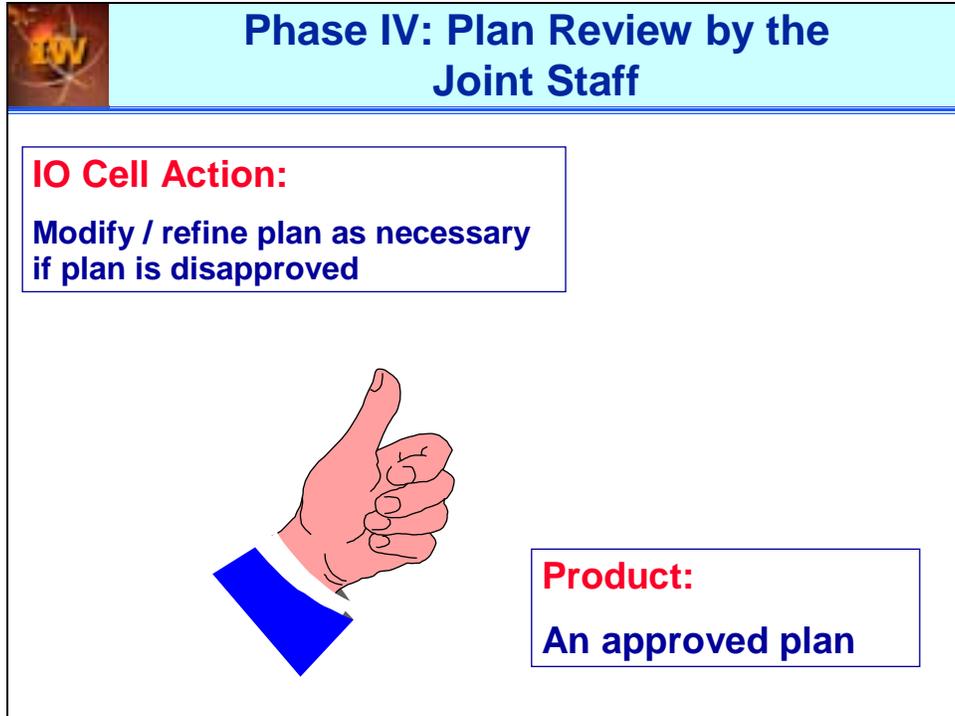
Develops complete IO plan and coordinates with appropriate staff sections, operational units, and supporting agencies for each of the IO capabilities and related activities



Product:

IO Appendix to Annex C and inputs to Annexes B, F, G, K, N, S, T, and V

This summarizes the IO Cell actions for Phase III of the Deliberate Planning Process. Once the plan is fully developed, the next phase begins ... the review of the OPLAN by the Joint Staff.



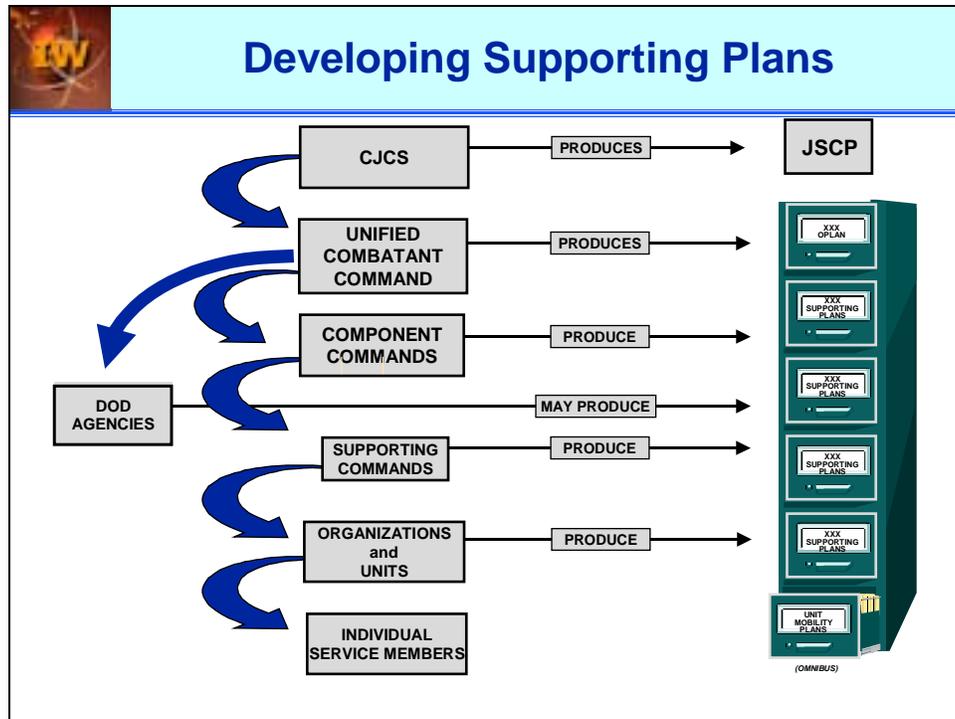
The graphic is a rectangular box with a light blue header and a white body. The header contains the text "Phase IV: Plan Review by the Joint Staff" in bold blue font. In the top-left corner of the header is a small square icon with a red and yellow background and the letters "JIP" in white. The body of the box contains three elements: a text box in the top-left with a blue border containing "IO Cell Action:" in red and "Modify / refine plan as necessary if plan is disapproved" in blue; a cartoon illustration of a hand in a blue suit sleeve giving a thumbs-up gesture in the center; and a text box in the bottom-right with a blue border containing "Product:" in red and "An approved plan" in blue.

Phase IV: Plan Review by the Joint Staff

IO Cell Action:
Modify / refine plan as necessary
if plan is disapproved

Product:
An approved plan

4.d. Phase IV of the Deliberate Planning Process is the Plan Review by the Joint Staff. If the plan is disapproved, modifications as noted by the Joint Staff will be made and the plan will be resubmitted. Once the plan has been approved by the Joint Staff, it's time for the final step of the Deliberate Planning Process.



4.e. Phase V (the final phase) of the Deliberate Planning Process is the Development of Supporting Plans. Supporting plans are normally developed by supporting Combatant Commands, Component Commands, and DoD agencies tasked to support the plan. Normally, these organizations will conduct parallel planning while the CC's staff is developing the OPLAN, so the process of developing supporting plans is usually well underway by the time the Joint Staff approves an OPLAN. The IO Cell should be prepared to aid in the development and review of supporting plans. Supporting plans should be submitted within 60 days of the Joint Staff approving an OPLAN. The supported CC approves supporting plans. Supporting plans will focus on:

- Mobilization
- Deployment
- Employment
- Sustainment
- Redeployment

The planners must consider IO to support each of these activities.



Phase V: Supporting Plans

IO Cell Action:

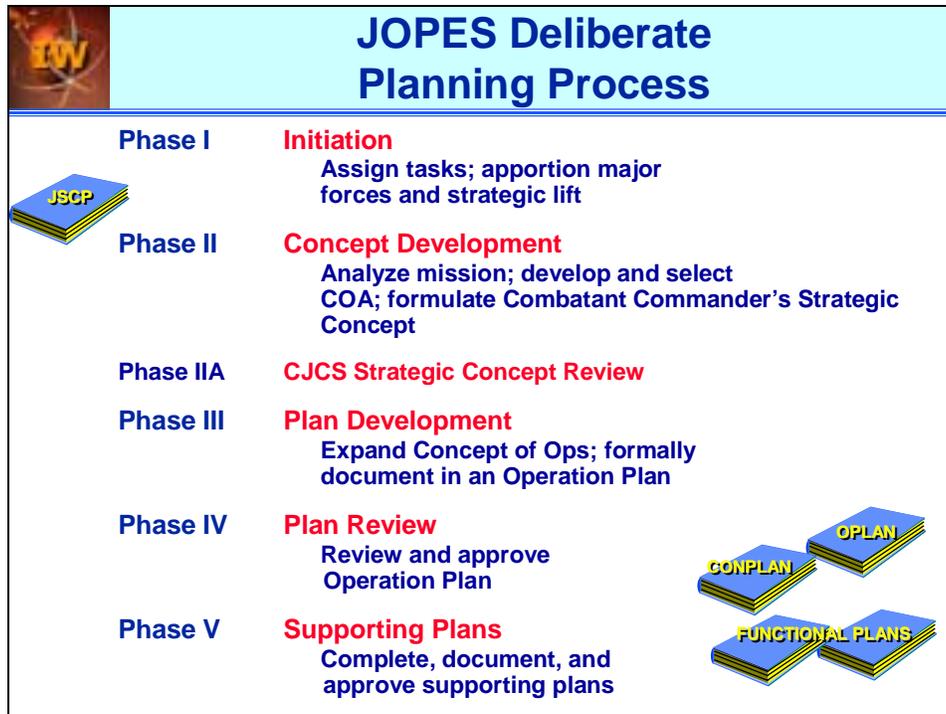
Coordinate / assist subordinates in preparing their own IO plans



Product:

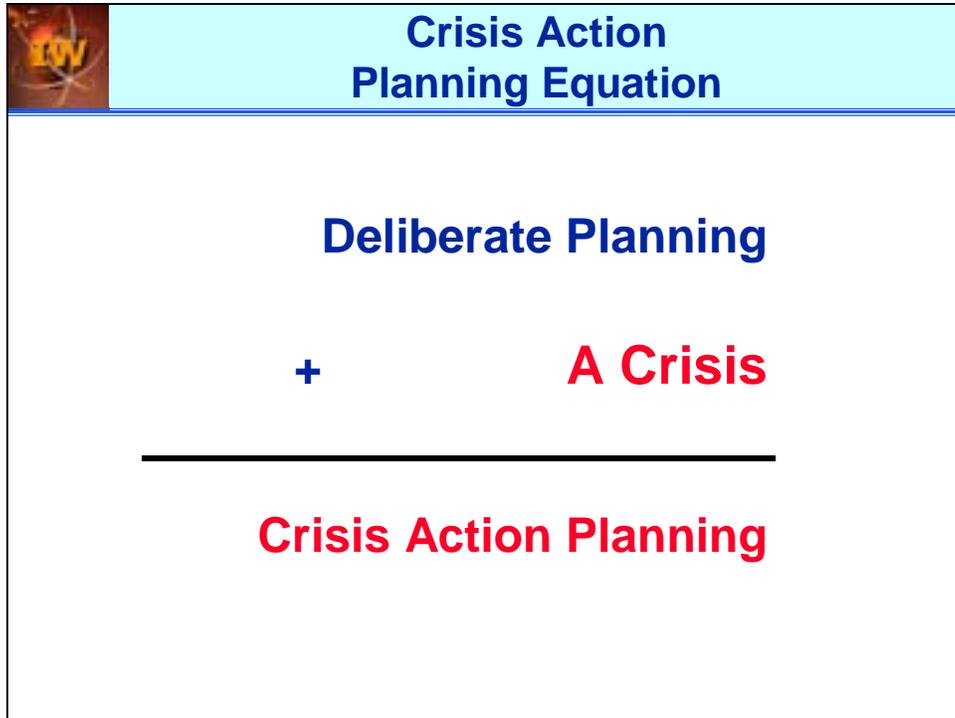
Supporting plans

This summarizes the IO Cell actions during the development of supporting plans.



5. Here is a review of the five phases of deliberate planning.

JOPES Crisis Action Planning Process



This is admittedly a simplification, but it illustrates the point that if you learn to do deliberate planning, you can flex to do crisis action planning.

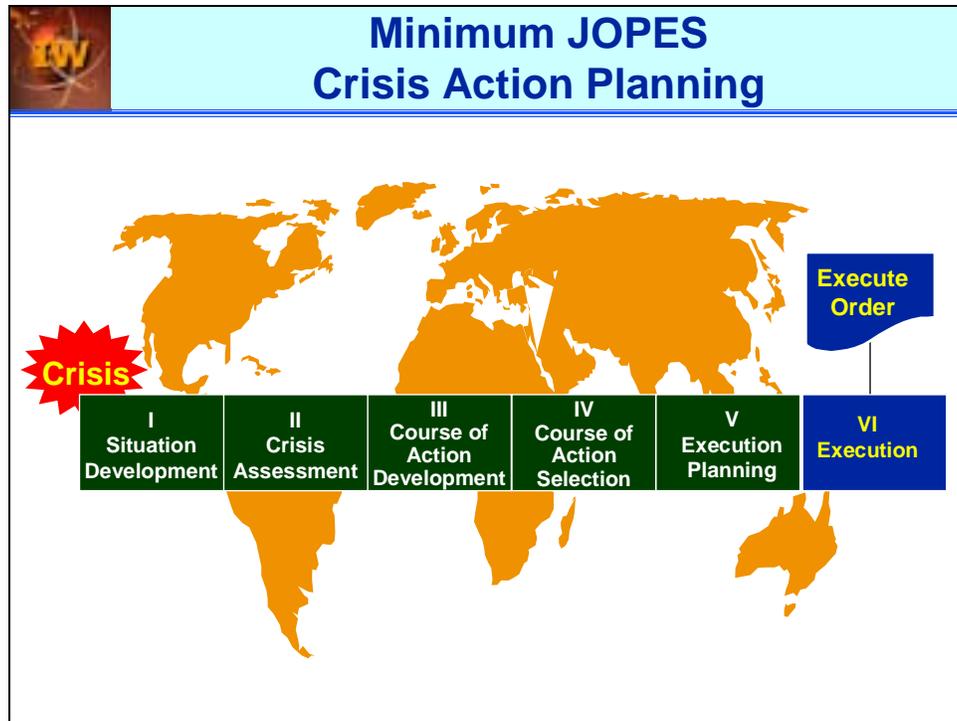
INFORMATION OPERATIONS PLANNING RELATED TO CRISIS ACTION PLANNING			
PLANNING PHASE	JOPES	IO CELL PLANNING ACTION	IO PLANNING OUTCOME
PHASE I	Situation Development	IO cell identifies planning information requirements as situation develops.	Tasking to gather/obtain required information.
PHASE II	Crisis Assessment	IO cell identifies information requirements needed for mission planning. IO cell assists in development of combatant commander's IO planning guidance to support overall operational planning guidance.	IO planning guidance. Initial liaison with units and agencies that may participate in or support IO operations.
PHASE III	Course of Action Development	IO cell supports the development of intelligence, operations, and communications staff estimates.	IO portion of staff estimates.
PHASE IV	Course of Action Selection	IO cell assists in transforming staff estimates into the Commander's Estimate. IO cell assists in the IO aspect of Combatant Commander's Concept as required.	IO portion of overall plan approved through CJCS.
PHASE V	Execution Planning	IO cell develops the complete IO plan and the plans for each of the IO elements in coordination with appropriate staff sections, operational units, and supporting agencies.	Approved offensive and defensive appendices with element tabs, completed supporting plans, and inclusion of IO requirements in TPFDD.
PHASE VI	Execution	IO cell monitors IO operations and adapts IO objectives to support changing operational directives.	IO objectives modified as necessary to support changing operational objectives.
CJCS = Chairman of the Joint Chiefs of Staff IO = Information Operations TPFDD = Time-Phased Force and Deployment Data			

IO Crisis Action Planning

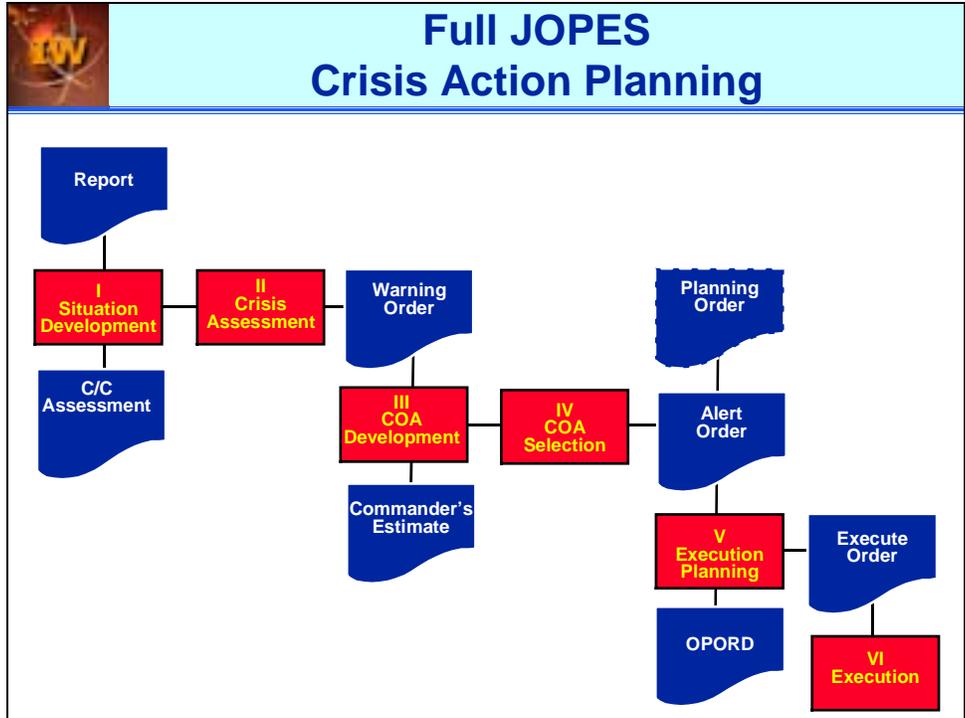
**Joint Pub 3-13
Page V-8**

The table is from JP 3-13 Figure V-4, page V-8.

In contrast to deliberate planning, crisis action planning normally takes place in a compressed time period. In crisis action planning, coordination of the IO plan is even more crucial than in deliberate planning. This section provides a general guide to IO planning as an integrated part of the JOPES crisis action planning at the combatant command level. This figure may be adapted as required for similar IO planning guidance at the subordinate joint force and component levels.



This is the absolute minimum execution flow that will occur during crisis action planning. An execute order is required for all circumstances.



6. Crisis Action Planning. In the beginning of this section, it was noted that Information Operations, by their very nature, do not lend themselves to Crisis Action (time-sensitive) planning. However, it is inevitable that some future situations will necessitate crisis action planning. So let's look at how we can adapt the IO Cell actions we used in deliberate planning in order to support crisis action planning.

6.a. Situation Development. Situation development may take place over a period of days, months or even years. It mainly entails intelligence personnel monitoring the situation in the CC's AOR, with a focus on the CC's priority intelligence requirements (PIRs) and with an eye for any developments with the potential to destabilize the AOR. If any of the developments in the AOR convince the CC that there is a potential crisis developing, the CC will issue an OPREP-3 report to through the JCS to the SECDEF, stating his assessment of the situation. At this stage, it's time for the IO Cell to begin monitoring the situation, identifying intelligence gaps necessary for IO and formulating RFIs to be submitted to the J2.

6.b. Crisis Assessment. After reviewing the CC's assessment, the SECDEF will either direct the CC to continue monitoring or they will issue a warning order through the JCS, directing the CC to begin planning. The warning order may prescribe one or more courses of action to be considered and will apportion forces to the CC for planning purposes. The IO Cell should submit its initial RFIs to the J2 upon receiving a warning order.

6.c. Course of Action Development. The staff will develop courses of action and produce Staff Estimates of Supportability as was discussed for Deliberate Planning. The IO Cell's actions for this process are the same as was discussed for Deliberate Planning. Unlike Deliberate Planning, however, the CC does not select the COA for Crisis Action Planning. Instead, a Commander's Estimate, describing each course of action and recommending a specific course of action is submitted to the SECDEF through the Joint Staff. The SECDEF will select the course of action.

6.d. Course of Action Selection. The SECDEF will select the course of action and then do one of three things. The first and most desirable option is to direct the CC to continue planning and to continue monitoring the situation. The second possibility is to issue an alert order, allowing all players involved in the operation to begin preparing to execute the mission. The last and least desirable possibility is that the SECDEF considers the situation so dire that they decide to issue an immediate execution order. In any event, as soon as a course of action is selected, the IO Cell must commence planning to produce a fully developed IO plan as was done in Deliberate Planning, developing the necessary synchronization matrices, IO planning worksheets, and execution checklists. Now let's take a look at executing the Operations Order (OPORD).

Executing the Plan

	<h3>Phase V Execution Planning</h3>
<p>IO Cell Action:</p> <p>Develops complete IO plan and coordinates with appropriate staff sections, operational units, and supporting agencies for each of the IO capabilities / related activities</p>	
	<p>Product:</p> <p>Strategy-to-Task Model, Synchronization Matrix, detailed plans, IO Appendix to Annex C and inputs to Annexes B, F, G, K, N, S, T, and V of OPORD</p>

6.e. Since the previous four planning steps are identical to deliberate planning, we will not go into more detail. With Phase V Execution Planning, we enter a realm that does not exist during deliberate planning. We are now able to add the detail, due to current events and real-time intelligence, which is not possible with an OPLAN.

	<h2>Phase VI Execution</h2>
<ul style="list-style-type: none">• IO Cell Action<ul style="list-style-type: none">– Via established feedback channels, monitor IO operations and adapt IO objectives and daily activities to support developments in the ever changing situation• Products<ul style="list-style-type: none">– Daily Execution Checklist and briefing products for the Combatant Commander	

6.f. Executing the OPLAN. The discussion in this section applies to both Deliberate and Crisis Action Planning. At some time in the future, it may be necessary to execute what was previously planned. In the case of Deliberate Planning, this will mean pulling a completed plan off of the shelf and converting it to an OPORD. For Crisis Action Planning, the execution is the last step of the process. In any case, at some point the staff will be required to convert their planning into OPORD and then to execute the OPORD. The following discussion covers the converting of IO planning into IO execution.



Executing the OPORD

IO cell representatives complete an IO Implementation Worksheet listing details of each IO action.

IO IMPLEMENTATION WORKSHEET					
Category (See Codes)	When (Date)	Action	Target(s)	Primary Themes (See Codes)	Purpose
1	14 Dec 96	Broadcast taped commentary from the Bosniac radio station in Tuzla every 2 hours	National-level Bosniac politicians; specifically Petro Drko, Minister of Refugees	DP1 & DP5	Use public opinion to pressure Bosniac officials to comply with the Dayton Peace Accord (DPA)
2	30 Jan 97	Distribute handbills in Tuzla, Garli & Tranbil	Bosniac mayors of Tuzla, Garli & Tranbil	DP2 & DP4	Encourage targets not to support Violent demonstrations

The IO Implementation Worksheet is used by members of the IO Cell to provide specific details on how they will implement the action reflected on the Synchronization Matrix

CATEGORY CODES

1. PSYOP RADIO MESSAGE (COMMENTARY)	10. CIVIL AFFAIRS
2. PSYOP RADIO MESSAGE (THEMATIC BURST)	11. JMC MEETING
3. PSYOP HANDBILL	12. JMC BILAT
4. PSYOP LOUDSPEAKER	13. 2D BRIGADE
5. PRESS CONFERENCE	14. TF 1/18
6. PRESS RELEASE	15. TF 1/26
7. PRESS GUIDANCE	16. IPTF
8. PUBLIC AFFAIRS RADIO SPOT	17. COMMAND GROUP
9. POLAD MEETING	

APPROVED THEMES

MESSAGES FOR PUBLIC OFFICIALS

MESSAGES FOR MILITARY LEADERS

MESSAGES FOR POLICE & SPECIAL POLICE

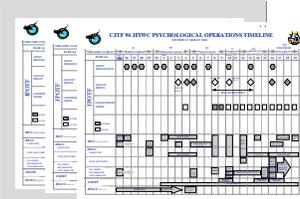
MESSAGES FOR THE GENERAL PUBLIC

As you see, the example identifies a specific date, target, and info themes

6.f(1) Building IO Execution Worksheets. Recall that during the OPLAN formulation, the IO cell developed IO synchronization matrices and IO planning worksheets (see above graphic) for each IO capability and related activity. In order to execute the IO plan, these must be converted to a daily IO Execution Worksheet. The first stage is to develop an execution sheet for each IO capability and related activity. Examples of a Daily IO Execution Worksheet are shown on the following two pages.



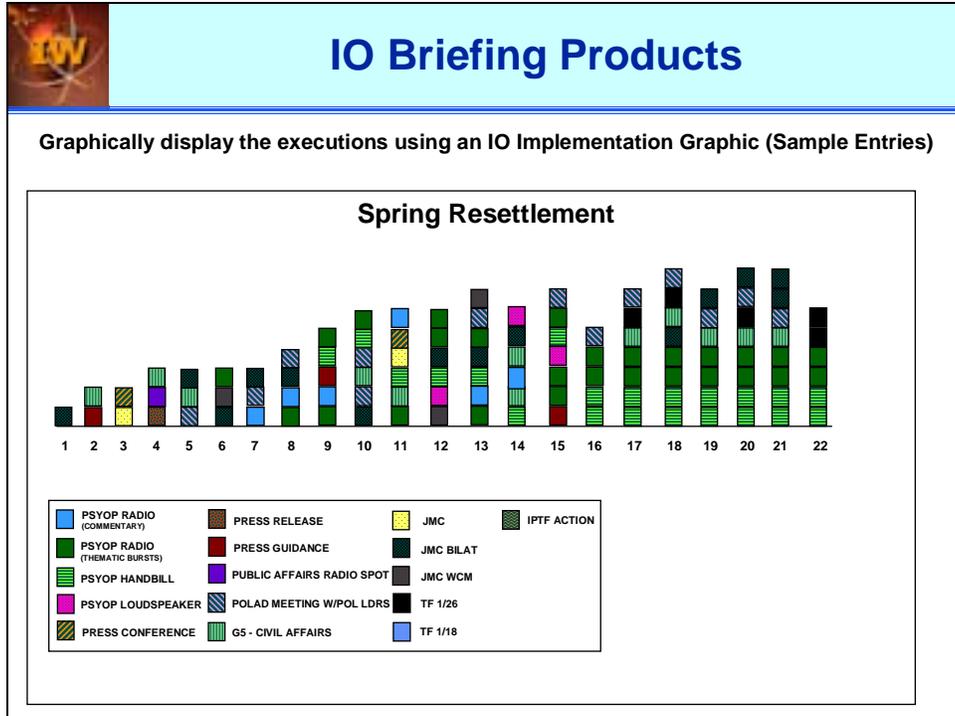
Execution Checklist



Convert the synchronized plan to an Executable Checklist

EVENT DESCRIPTION	EVENT TYPE	DATE	LOCATION	
PSYOP Radio Broadcast	National PSYOP	4/26/96	Various	National. Check with
PSYOP Radio Broadcast	National PSYOP	4/27/96	Various	National. Check with
PSYOP Radio Broadcast	National PSYOP	4/28/96	Various	National. Check with
PSYOP Radio Broadcast	National PSYOP	4/30/96	Various	National. Check with
SOF DA against PCL pump station	DA001/C2/W01	5/1/96	Ft. Pickett, VA	SOF support to JFIV
PSYOP Radio Broadcast	National PSYOP	5/1/96	Various	National. Check with
EP-3E on Station	Non-organic ES	5/2/96	As Assigned	Liaise with C2W cell
Air SUPREQ for MC-130 Mission (3 May)	ATO Input	5/3/96	Camp Blanding	Input to JFACC for 3
Air SUPREQ for TARPS missions over false BLS	NA	5/3/96	Cape Hatteras	6 May ATO
ARSOF DA against fiber optic node	DA002/C2/W02	5/3/96	Harvey Pt, N.C.	ARSOF support to J

6.f(2) The execution worksheet is used to monitor the progress of daily IO activities. As each event on the worksheet is executed, the worksheet should be so annotated. Any show stoppers must be highlighted on the daily worksheet and particular attention should be given to these activities, as the J3 and other affected staff elements will have to be notified whenever a show stopper IO event is not executed as planned.



6.g. IO Briefing Products. It will be necessary for the IO Cell to develop briefing products to periodically update the Commander on IO activities. There is no prescribed method to do this. Local SOP will probably direct the briefing method and products with guidance from the J3. The example shown in the graphic above is a method developed by a 11OC (Land) field support team in Bosnia.



IO Feedback

Aggressively seek feedback and update IO plans



*Gathering feedback
is a continuous process*

Sources

- HUMINT, PSYOP and Civil Affairs Teams
- Open Source Intelligence (OSINT)
- Internet (Newsgroups, etc.)
- SIGINT
- Contact with the public
- Press inquiries and comments
- DoS Bureau of Intelligence and Research (INR) surveys
- FBIS reporting
- NGOs, PVO, International Organizations
- POLAD meetings
- Intel assessments

6.h. Monitoring the Success of the IO Campaign. Finally, it is incumbent upon the IO Cell team to monitor feedback on the success of the IO campaign. Feedback may come from a myriad of sources, only a few of which are shown in the graphic above. Developing metrics by which to assess the effectiveness of IO activities is a difficult task and an area in which little work has been done to date. Primary emphasis must be on conducting initial assessments for the purpose of making immediate adjustments to the daily IO execution checklist. The more difficult task, however, is to monitor the effectiveness of the IO campaign over time to ensure that it promotes the CC's vision and objectives.

This is the only available method of determining if your IO plan is working. The feedback should be very closely linked with the measures of effectiveness. Other possible ideas include:

- Pre-established contracts with local (host-nation) polling organizations
- Others?

This page intentionally left blank

Chapter V – Joint Information Operations Attack Planning Process

The Joint Forces Staff College would like to thank the Joint Information Operations Center for providing the materials for this chapter. Slides illustrating main points start at page V-19.

Introduction

The Joint Information Operations Attack Planning Process (JIOAPP) is a five-step method for conducting Information Operations (IO) Attack Planning. The JIOAPP is part of the Joint IO Planning Process (JIOPP), which includes, in addition to the JIOAPP, the Joint IO Defensive Planning Process (JIODPP). The JIOPP provides a logical, structured method for integrating Information Operations planning into the Joint Operations Planning process.

The JIOAPP facilitates planning at two levels – that conducted by the Unified Commands, as well as the subordinate Component Commands. Unified Command IO Planning usually has as its objective the construction of detailed IO task statements that are provided to the Components for further planning. Component-level planning strives to determine the optimum match between the Combatant Commanders Objectives and targets, as well as IO Assets (weapons) and targets. Since the IO planning process is information-intensive, it can also be highly collaborative in nature. Thus, information and expertise from sources and staffs outside the IO Planning Cell will probably be needed to apply the JIOAPP most effectively. Further, the responsibility for conducting contingency planning is shared among the Unified Commands and their Components, the Joint Chiefs of Staff, and Department of Defense Agencies and Centers. The CCs of the various Unified Commands bear the primary responsibility for executing those plans and therefore have the lead in plan development. The Joint Information Operations Center (JIOC) assists the Unified Command staffs in developing IO concepts, integrating these into contingency plans, and assisting in their execution.

The guidelines presented above regarding the roles of and boundaries between Unified Command, Component, and other planners may regularly shift. Planners at all levels should not hesitate to contact persons or staffs (or consult on-line sources) that can provide or acquire needed information, because at some point in this collaborative process, your expertise will be solicited as well!

The following information will assist you in using the JIOAPP to conduct IO planning in support of CC objectives. The purpose of each form will be explained and amplifying information provided as needed to help you complete the form. Because each planning situation is different, more forms than are provided in the initial package may be needed to complete a particular step. If more forms are needed, they can be easily acquired.

The Five Steps of the Joint Information Operations Attack Planning Process

The five major steps of the JIOAPP are listed below. There are a series of sub-steps associated with each of the major steps. The Steps and Sub-steps are as follows.

1. Refine the IO Objectives

- a. Review CC planning guidance. Identify specific CC objectives.

- b. Review and adjust, as necessary, IO related specified, implied, and essential tasks. Adjust IO objectives developed during mission analysis to ensure that the IO objectives support the CC's mission, concept of operations, objectives and end state.
- c. Pair IO objectives with IO methods and techniques that may help accomplish the objectives.
- d. Select the IO objectives that can play a significant role in accomplishing the CC's objectives.
- e. Determine timing / phasing of IO Objectives.
- f. Derive and write IO Sub-objectives as necessary based on selected IO methods and techniques, opposition centers of gravity (COG), and critical vulnerabilities (CV) that IO methods and techniques can affect.
- g. Time / phase IO Sub-objectives as required.

2. Generate the IO Tasks Associated with IO Objectives and Sub-objectives

- a. Identify the opposition Activity(ies) that, if affected, will help accomplish the associated IO Objectives/Sub-objectives
- b. Identify the Functions that most contribute to the opposition's conduct of the Activity
 - (1) Evaluate the Functions to determine their importance to the Activity's success; select the most important Functions
- c. Identify the Effects desired on the selected Functions
- d. Deconflict the Effects desired on the selected Functions
- e. Identify the Capability most suitable to achieve the Effect desired on the selected Functions
- f. Write and establish phasing for an IO Task Statement based on: opposition Activity and Function selected, Effect desired, and Capability to be applied to achieve the Effect
- g. Determine which Functional area and Component has the best capability to accomplish the IO Task/Sub-task; distribute the IO task to the Component(s)

3. Identify the IO Targets

- a. Identify the IO targets – characterized as hardware, software, wetware or data targets – which can be attacked to achieve the Effect desired on the opposition Function
 - (1) Evaluate and select the hardware, software, wetware and data targets associated with the Function to identify the ones most critical to the Function's success
 - (2) Evaluate the selected targets further to identify the ones most vulnerable to attack
- b. Confirm or refine Effects desired on selected targets
- c. De-conflict Effects desired on selected targets

4. Identify the IO Assets, derive the IO Sub-tasks, and prepare the candidate Master IO Target List

- a. Identify the IO Assets most appropriate for achieving the Effect desired on selected critical and vulnerable IO targets
 - (1) Evaluate the selected IO targets against the IO Assets most capable of achieving Effect desired; select Asset-Target pairs
- b. Evaluate selected Asset-Target pairs in light of cost-risk-benefit criteria to derive and write IO Sub-tasks
- c. Prepare the candidate Master IO Target List

5. Conduct Equity Review

- a. Review IO Sub-tasks in light of appropriate checklists to ensure various equities are properly considered

FORMS – GENERAL INSTRUCTIONS: To facilitate planners' ability to orient them when using this "paper process," the top of each form will display the major step of the JIOAPP to which the form pertains. The bottom of the form will display a sentence succinctly stating what information is to be recorded on the form.

Step One: Identify the Offensive Information Operations Objectives

FORM 1. Identify the IO Objectives. **Write the CC Objectives.** The purpose of this form is to record the CC objectives. In many instances, the IO planning cell will be *provided* the CC Objectives. In other cases, the IO Planning Cell may be involved in *deriving* the CC Objectives. The exact way by which CC Objectives will be determined will probably vary by CC staff and conflict scenario. The most important point here is to capture and record *all* CC Objectives.

FORM 2. Identify the IO Objectives. **Identify Specified, Implied and subsidiary tasks associated with the CC Objectives.** The purpose of this form is to record the Specified, Implied and subsidiary tasks. Upon receipt of a mission, the commander (in concert with his staff) begins his mission analysis by asking himself specific questions about higher headquarters or SECDEF purpose, intent, the area of operations, available assets, constraints, restrictions, risk, and time. The commander will subsequently disseminate the results of his analysis in his restated mission description, objectives, and concept of operations. The staff continues the mission analysis by asking additional questions, the most important of which is:

"What tasks must the command perform to accomplish the assigned mission successfully?"

To answer this question, extract all (with no consideration of IO) specified, implied or subsidiary tasks from the commander's objectives, concept of operations, mission statement and rules of engagement.

SPECIFIED TASKS are those tasks the commander spells out in the mission description, his operational objectives, his concept of operations and other guidance. They are what the commander wants accomplished.

IMPLIED TASKS are those additional major tasks that are necessary to accomplish the mission, but which are not specifically spelled out in the commander's guidance. They should not be routine, standing operating procedure-type tasks, or inherent responsibilities of the commander; e.g. providing flank protection for his own unit. Limit the implied tasks to major tasks that are "essential" to the accomplishment of the mission. Use available task lists (Uniform Joint Task List, Mission Essential Task List, etc.) to assist in this process.

SUBSIDIARY TASKS are any other tasks that could be viewed as supporting the mission.

FORM 3. Identify the IO Objectives. **Pair Specified, Implied and subsidiary tasks with IO Methods and Techniques that may help accomplish the tasks.** In this step, first examine the specified, implied and subsidiary tasks to determine what role IO may be able to play in accomplishing the tasks. Ask: can the IO methods and techniques listed on the form help accomplish the tasks? Pair specified, implied and subsidiary tasks with the IO Method or Technique that can best help accomplish the task, and enter these on the form along with the task.

FORM 4. Identify the IO Objectives. **Evaluate the Tasks according to the criteria.** The next step is to evaluate how well the specified/implied/subsidiary tasks can be accomplished using IO methods and techniques. To do this, assess the ability of IO Methods and Techniques to help accomplish the designated task according to these criteria: **Capability, Feasibility, Constraints** and **Adversary Vulnerability**.

CAPABILITY = Degree to which IO has the capability to accomplish or support the objective. Capability has two sub-components that can be considered when making the assessment. These are:

EFFICIENCY = Efficiency of IO in accomplishing the mission;

SUCCESS = Probability of success associated with IO in achieving the objective.

RATING SYSTEM for Capability

LOW = IO cannot accomplish or support accomplishment of the objective.

MEDIUM = IO may be able to accomplish or support accomplishment of the objective.

HIGH = IO can definitely accomplish or support accomplishment of the objective.

CONSTRAINTS = Degree to which constraints favor use of IO. Constraints have three sub-components that can be considered when making the assessment. These are:

POLITICAL = Degree to which political constraints favor use of IO

RULES OF ENGAGEMENT = Degree to which ROE favor use of IO

CULTURAL = Degree to which cultural (religion, etc.) constraints favor use of IO

RATING SYSTEM for Constraints

LOW = constraints preclude the use of IO.

MEDIUM = constraints permit the use of IO.

HIGH = constraints cause preference for use of IO.

FEASIBILITY = Degree to which IO is a feasible method for accomplishing or supporting the objective. Feasibility has three sub-components that can be considered when making the assessment. These are:

TECHNICAL = Technical feasibility of IO method/technique against opposition information and information processes

RESOURCES = Degree to which resources are available to implement IO capabilities

TIME = Degree to which sufficient time exists to implement and achieve IO results

RATING SYSTEM for Feasibility

LOW = using IO is NOT feasible.

MEDIUM = using IO may be feasible.

HIGH = using IO is feasible.

ADVERSARY VULNERABILITY = Degree to which adversary is vulnerable to IO capabilities.

RATING SYSTEM for Adversary Vulnerability

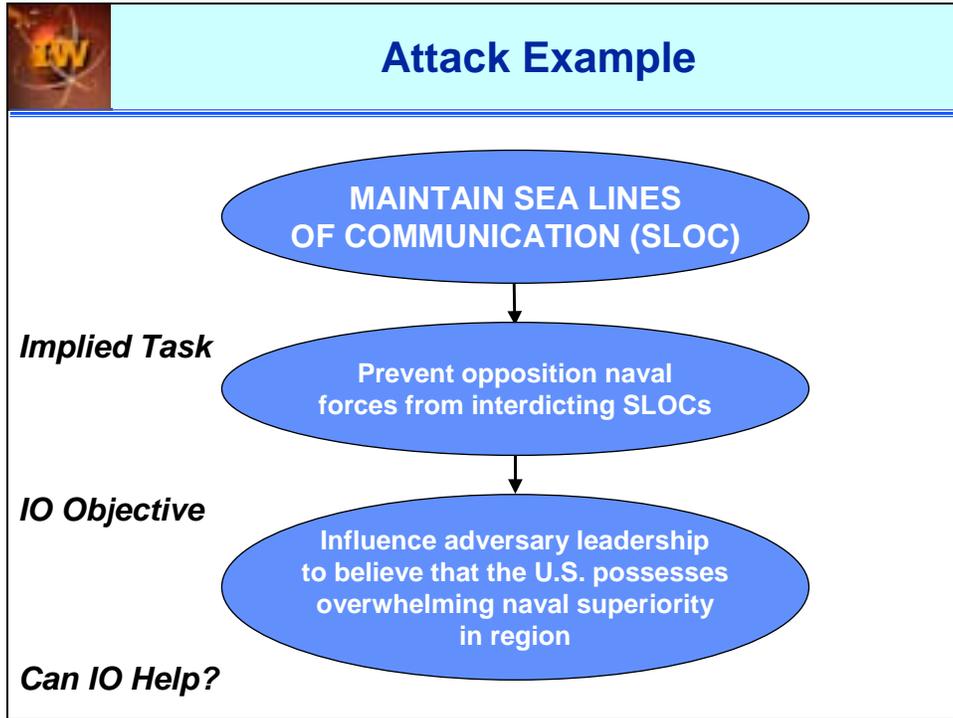
LOW = vulnerability to IO capabilities is limited

MEDIUM = moderately vulnerable to IO capabilities

HIGH = extremely vulnerable to IO capabilities

Evaluate the list of specified, implied and subsidiary tasks against the provided criteria to determine the applicability of IO to successful task accomplishment. Use the weighting scheme provided (Default scheme is: Capability, Feasibility, Constraints and Vulnerability are weighted at .25 each; the value for Low = .2; Medium = .5; and High = .8) to make the calculations indicated on the form to arrive at a numerical total. The higher the total, the greater the potential contribution of IO is to accomplishing the task. Choose the highest value tasks for continued planning.

FORM 5. Identify the IO Objectives. **Write an IO Objective statement for Tasks selected.** Enter the IO Objective Statement on the form. The IO Objective statement should clearly indicate how an IO method or technique, or the Effect created by an IO Method or Technique, would accomplish or help accomplish the specified, implied or subsidiary task. The IO Objective statement can include the general target class or audience to be impacted, and may state what the desired outcome may be. An example is shown in the following chart:



SAMPLE IO OBJECTIVE DERIVATION

FORM 6. Identify the IO Objectives. **Establish time phasing of IO Objectives.** On this form, assign the accomplishing of IO Objectives to the desired phase of the campaign. Assign start and end dates for the IO Objective and reference the phasing in relation to D-Day. The opportunity will be provided to review and refine the phasing data throughout the planning process.

FORM 7. Identify the IO Objectives. **Derive and write IO Sub-objectives as necessary.** NOTE: *The derivation of IO sub-objectives is optional.* Sometimes, the further breakdown of IO Objectives into sub-objectives is warranted to identify more specifically impacts desired or to delineate target classes further. Continuing the example given in the chart for Form 5, an IO Sub-objective could perhaps specify distinct groups to influence within the opposition leadership – the intelligence leadership or the foreign ministry leadership. The sub-objective derivation would consider the IO Methods and Techniques available and the opposition centers of gravity that are vulnerable to these. Any IO Sub-objectives derived should be phased.

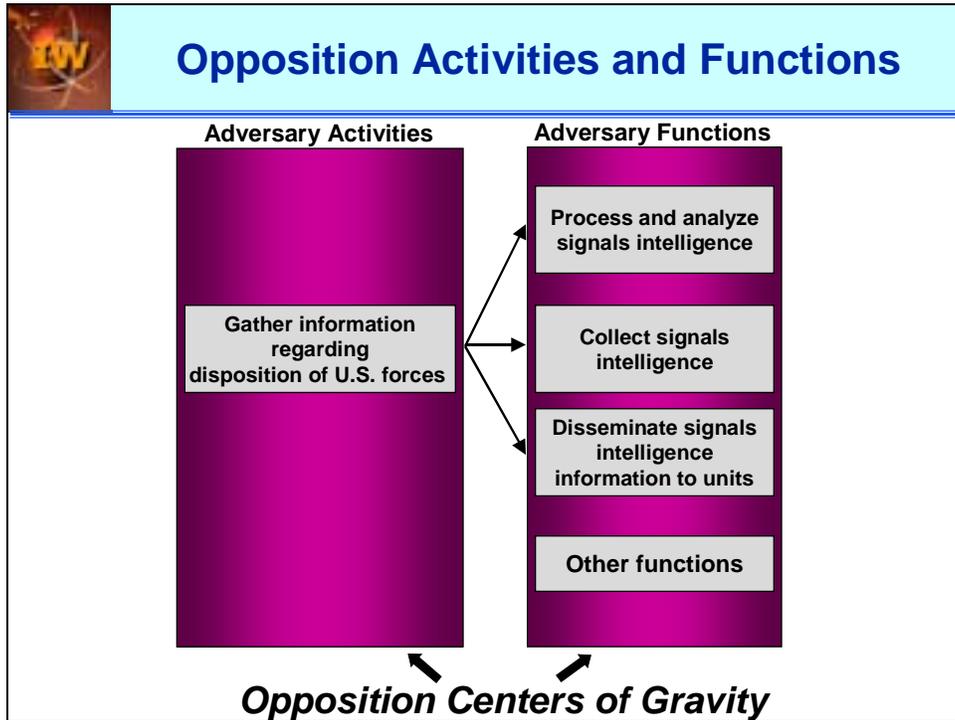
Step Two: Generate the Offensive Information Operations Tasks

FORM 8. Generate the IO Tasks. **Examine the IO Objectives/Sub-objectives and consider what opposition Activities will be affected.** On this form, list opposition **Activities** to be affected by friendly IO. There are two techniques that can be employed when trying to identify the best opposition Activities to affect. **The first technique departs from the perspective of a friendly IO planner.** This planner

knows the friendly IO Objective to be achieved, and asks, "To which adversary Activity (where in the adversary "system") must I apply IO Methods and Techniques to achieve the IO Objective?" **The second technique involves the friendly IO planner assuming the role of the adversary.** Using this technique, the planner speculates that adversary planners have anticipated the friendly IO Objectives, and will take necessary steps to thwart their accomplishment. Using this technique, the friendly planner assuming the adversary role asks "what Activities would the adversary conduct if they anticipated the friendly IO Objective and wanted to defeat it? I will generate my IO tasks to affect those adversary Activities." Either technique, or the two in combination, may be employed to select opposition Activities to be affected by friendly IO.

FORM 9. Generate the IO Tasks. **Identify the Functions that most contribute to the Opposition's conduct of the Activity.** An Activity can be broken down into its component parts, known as "**Functions**" in the JIOAPP. The successful accomplishing of the adversary activity will depend more on some of these Functions than on others. On this form, list those Functions that most contribute to the adversary's successfully accomplishing the Activity. *It is these Functions that friendly IO strives to affect.* Refer to the chart below to see examples of Functions associated with an Opposition Activity.

FORM 9A. Generate the IO Tasks. **Evaluate the Functions to identify those that contribute most to the Activity's success.** *This is an optional step.* To evaluate the Functions, use these criteria: **Contribution, Impact, and Uniqueness.**



CONTRIBUTION = Contribution made by the Function to the successful conduct of the activity. Contribution has two sub-components that can be considered when making the assessment; these are:

ROLE = Role the Function plays in accomplishing an Activity
VALUE = Value the Function adds to accomplishing an Activity

RATING SYSTEM for Contribution

LOW = The Activity can be successfully accomplished without the Function.

MEDIUM = The Activity's success would be hindered without the Function.

HIGH = The Activity cannot be successfully accomplished without the Function (is required for successful accomplishment of the Activity).

IMPACT = Degree to which the mission and/or economic impact resulting from the loss of the Function affects the adversary's ability to conduct the selected Activity. Impact has two sub-components that can be considered when making the assessment; these are:

ECONOMIC = The cost associated with loss of the Function in terms of lost investment, reconstitution cost, etc.

MISSION = Degree to which mission can be completed without execution of the Function

RATING SYSTEM for Impact

LOW = No or marginal impact on the opposition's ability to accomplish its Activity.

MEDIUM = Moderate impact on the opposition's ability to accomplish its Activity.

HIGH = Severe impact on opposition's ability to accomplish its Activity.

UNIQUENESS = Degree to which the Function is one-of-a-kind or can be readily duplicated, and/or the degree to which it can be recovered if loss occurs. Uniqueness has two sub-components that can be considered when making the assessment; these are:

REDUNDANCY = Degree to which the Function is one-of-a-kind

RECOVERABILITY = Degree of difficulty associated with recovering the Function after a loss occurs in time to contribute to accomplishment of the Activity

RATING SYSTEM for Uniqueness

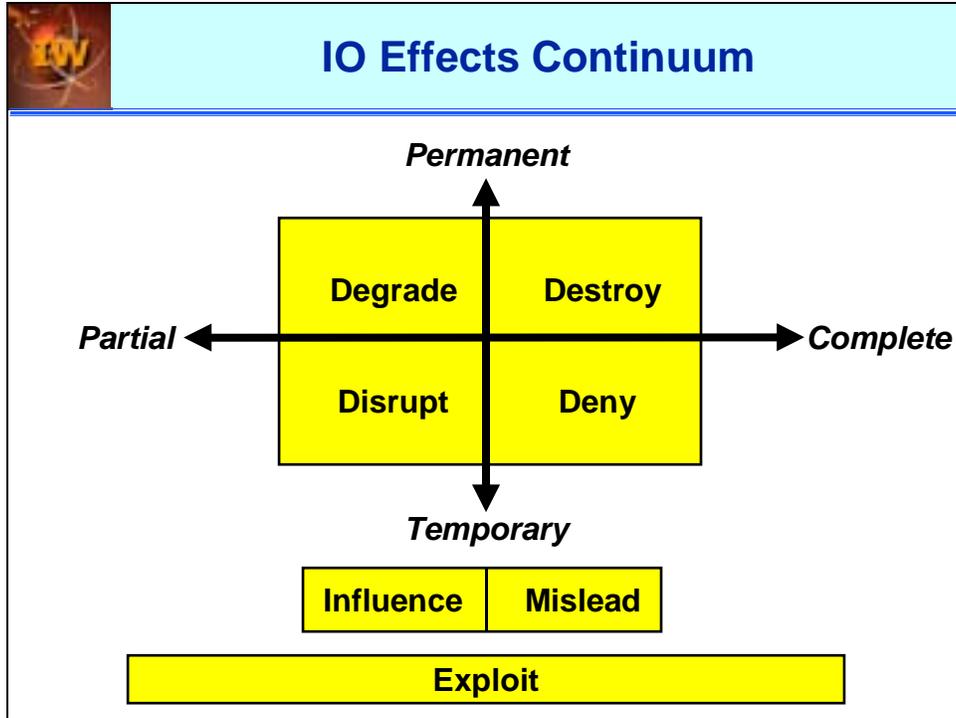
LOW = the Function is highly redundant and/or easily recovered.

MEDIUM = the Function is moderately redundant and/or it can be recovered with moderate effort within the required time frame.

HIGH = the Function is one-of-a-kind and/or it cannot be recovered in the required time frame.

Use the weighting scheme provided (Default scheme is: Contribution, Impact, and Uniqueness are weighted at .33 each; the value for Low = .2; Medium = .5; and High = .8) to make the calculations indicated on the form to arrive at a numerical total. The higher the total, the more important the contribution of the Function is to the Activity's success.

FORM 10. Generate the IO Tasks. **Identify the Effect desired on the selected Functions.** On this form, select the Effect desired on the opposition Functions. The types of Effects are displayed on the form and are explained below.



Destroy = Damage done to the Function is permanent, and all aspects of the Function have been affected **OR** A Function's operation is permanently impaired, and the damage extends to all facets of the Function's operation.

Deny = Damage done to the Function is only temporary, but all aspects of the Function were affected **OR** A Function's operation is impaired over the short term, but the damage extends to all facets of the Function's operation.

Degrade = Damage done to the Function is permanent, but only portions of the Function were affected; that is, the Function still operates, but not fully **OR** A Function's operation is permanently impaired, but the damage does not extend to all facets of the Function's operation.

Disrupt = Damage done to the Function is temporary, and only portions of the Function were affected **OR** A Function's operation is impaired over the short term and the damage does not extend to all facets of the Function's operation.

Mislead = creation of a false perception which leads the opposition to act in a manner detrimental to mission accomplishment while benefiting accomplishment of friendly objectives.

Influence = selected projection or distortion of the truth to persuade the opposition to act in a manner detrimental to mission accomplishment while benefiting accomplishment of friendly objectives.

Other = There may be other Effects desired, and this field is designed to allow for "write in" Effects.

FORM 11. Generate the IO Tasks. **De-conflict the Effects desired on the selected Function.** This form allows you to review and de-conflict the effect(s) assigned to each opposition Function. The most important part of this form is your careful scrutiny of each Effect for accuracy and conflicts.

1. Review each opposition Function and determine if the selected Effects are correct and desirable. Remember that the form should reflect your choices correlated with one of the six standard verbs (disrupt, degrade, deny, destroy, mislead and influence) or your write-in selection. These "Effect

verbs" will become part of the applicable IO Task Statement.

2. Next, review your selections for opportunities to synchronize effects. You should be thinking here, as you will later on when examining available Elements, about the relative merit of sequencing IO effects (e.g., mislead, then destroy) or "massing" on the IO objective/target. Massing in this context infers a mutually supporting strategy to use different Effects in rapid sequence to confuse or delay adversary response. Remember that having multiple Effects on Functions is acceptable, and may in fact be desirable. Make sure, however, that the Effects do not conflict with each other (for example, insure that the Effects are induced in different phases of the campaign), and are induced in the desired order (for example, it's difficult to induce a Mislead Effect on a target already Destroyed!).

FORM 12. Generate the IO Tasks. **Identify the Capability most suitable to achieve the Effect desired.** On this form, list the Function to be affected and the Effect desired. Now select the IO Capability most suitable for achieving the desired Effect.

There are general groupings of IO Elements capable of producing Effects desired.

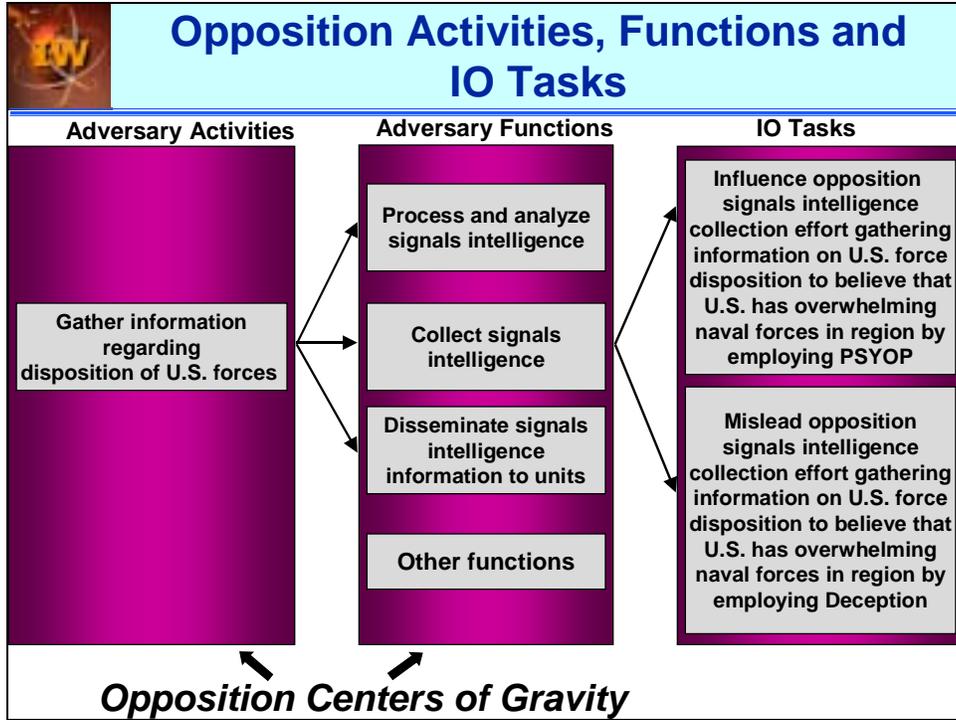
Deception Elements will cause the **Mislead** Effect.

PSYOP Elements will induce the **Influence** Effect.

Destruction Elements (concussion – bombs; kinetic – bullets; or radio frequency – pulse) can cause the Destroy Effect (**NOTE:** There are other Elements that can cause the **Destroy** Effect as well).

Deny, Disrupt and **Degrade** Effects can be achieved using **Destruction** Assets applied precisely to the portion of the adversary Function to be affected. Also, for example, electronic jamming (EW Capability) of a transient nature may induce the **Deny** or **Disrupt** Effects on adversary Functions. A high power radio frequency pulse or laser pulse (EW Capability) may induce a **Degrade** Effect. Computer Network Attack Elements might possibly induce multiple Effects separately or sequentially.

FORM 13. Generate the IO Tasks. **Write the IO Task Statements.** On this form combine the Opposition Activity and Function to be affected, the Effect desired, and the IO Capability that is most suitable for achieving the Effect and combine them to write an IO Task Statement. The chart shows examples of properly completed IO Task Statements.

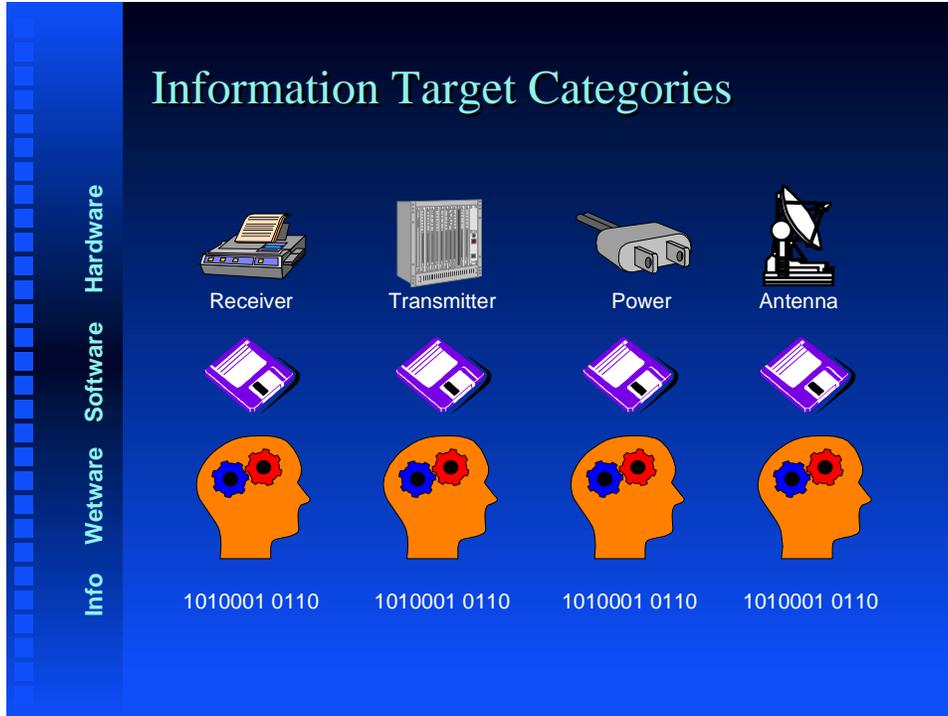


FORM 14. Generate the IO Tasks. **Assign the IO Tasks to the Components.** On this form, write in the IO Tasks. Determine primary and supporting responsibilities (e.g., Army primary, Air Force supporting). Fill in the Function blocks associated with the tasks by entering the Component selected and a "P" or an "S" to denote primary or supporting. Example: under the Deception Heading for Task 1 would be "Navy - P" if the Navy were the most appropriate/capable Component to accomplish the IO Task. If supporting responsibilities were to be assigned, this notation would also be made in the block, e.g., "Air Force - S."

Step Three: Identify the Information Operations Targets

Form 15: Identify the IO Targets. **Identify the IO Targets – characterized as Hardware, Software, Wetware or Data targets – that can be attacked to achieve the Effect desired on the opposition Function.** On this form, write in the hardware, software, wetware or data targets associated with the Function to be attacked. Target selection is, more often than not, a collaborative process. The participants in the process may include the J3, J2T, the Services, agencies such as the Joint Warfare Analysis Center and Information Operations Technology Center, and others.

Many factors must be assessed when selecting targets. Ideally, the targets identified for further analysis should be known to play an important role in the successful operation of the Function to be affected. The following chart illustrates the generic types of targets that can be found in the hardware, software, wetware and data categories.



FORM 16: Identify the IO Targets. Evaluate and select the hardware, software, wetware and data targets associated with the Function to identify the ones most critical to the Function's success; evaluate further to identify the ones most vulnerable to attack. Determining how critical a given target is to a Function's success should include an examination of three factors:

- What is the **contribution** of this target to the successful operation of the Function?
- What would be the **impact** on the successful operation of the Function if the target were struck?
- How **unique** is the target's contribution to the Function's successful operation?

Determining how **vulnerable** a target is should include an examination of another three factors:

- Is the target **accessible**?
- Is the target **susceptible** to attack?
- Is it **feasible** to attack the target?

After evaluating targets in each of the categories as to their criticality and vulnerability, select the ones desired and write them on the form.

FORM 16A: Identify the IO Targets. Evaluate and select the hardware, software, wetware and data targets associated with the Function to identify the ones most critical to the Function's success; Evaluate further to identify the ones most vulnerable to attack. *This is an optional step.* Criteria-based analyses can be done on this step if desired. To refine the evaluation and selection of the targets most critical to the Function's success as well as most vulnerable, apply the same criteria used in **STEP 9A**, plus the vulnerability criterion, but this time to targets. To evaluate the targets, use these criteria: **Contribution, Impact, Uniqueness, and Vulnerability.**

CONTRIBUTION = Contribution made by the Target to the successful conduct of the Function. Contribution has two sub-components that can be considered when making the assessment; these are:

ROLE = Role the Target plays in accomplishing the Function
VALUE = Value the Target adds to accomplishing the Function

RATING SYSTEM for Contribution

LOW = The Function can be successfully accomplished without the Target.

MEDIUM = The Function's success would be hindered without the Target.

HIGH = The Function cannot be successfully accomplished without the Target (is required for successful accomplishment of the Function).

IMPACT = Degree to which the mission and/or economic impact resulting from the loss of the Target affects the adversary's ability to conduct the selected Function.

Impact has two sub-components that can be considered when making the assessment; these are:

ECONOMIC = The cost associated with loss of the Target in terms of lost investment, reconstitution cost, etc.

MISSION = Degree to which mission can be completed without execution of the Target

RATING SYSTEM for Impact

LOW = No or marginal impact on the opposition's ability to accomplish its Function.

MEDIUM = Moderate impact on the opposition's ability to accomplish its Function.

HIGH = Severe impact on opposition's ability to accomplish its Function.

UNIQUENESS = Degree to which the Target is one-of-a-kind or can be readily duplicated, and/or the degree to which it can be recovered if loss occurs. Uniqueness has two sub-components that can be considered when making the assessment; these are:

REDUNDANCY = Degree to which the Target is one-of-a-kind

RECOVERABILITY = Degree of difficulty associated with recovering the Target after a loss occurs in time to contribute to accomplishment of the Function

RATING SYSTEM for Uniqueness

LOW = the Function is highly redundant and/or easily recovered

MEDIUM = the Function is moderately redundant and/or it can be recovered with moderate effort within the required time frame

HIGH = the Function is one-of-a-kind and/or it cannot be recovered in the required time frame

VULNERABILITY = Degree to which a Target is "open" to attack. Vulnerability has three sub-components that can be considered when making the assessment; these are:

ACCESSIBILITY = Degree to which the Target can be "reached" by an attacking system

FEASIBILITY = A measure of the feasibility associated with the attacking of the target

SUSCEPTIBILITY = Degree to which the Target is susceptible to attack

RATING SYSTEM for Vulnerability

LOW = Target is open to attack only to a limited degree at best

MEDIUM = Target is open to attack

HIGH = Target is very open to attack

Use the weighting scheme provided (Default scheme is: Contribution, Impact, Uniqueness and Vulnerability are weighted at .25 each; the value for Low = .2; Medium = .5; and High = .8) to make the calculations indicated on the form to arrive at a numerical total. The higher the total, the more important the Target is in assuring the Function's success.

FORM 17: Identify the IO Targets. **Confirm or Refine Effects desired on targets selected.** Use this form to confirm or refine the effects desired on the targets selected. The form contains analysis aids that facilitate planners' review of Effects and allow the charting of "influence paths" when mapping the relationships among potential wetware targets. Use the "IO Effects" chart as an aid to confirm or refine Effects desired on selected targets. Use the "Derive Actor" chart to map command or reporting relationships between echelons or hierarchies, or within high-level staffs. After the review, complete the form by writing in the targets selected and the corresponding Effect desired.

FORM 18: Identify the IO Targets. **De-Conflict Effects desired on selected targets.** On this form, write the targets selected along with the Effects proposed for each. Insure the Effects do not conflict with each other (e.g., targets selected for both Influence and Destroy Effects) or that, if conflicts do exist, they are acceptable (e.g., a target is slated for two Effects, Influence from D -1 to D +2, and then Destroy on D +3).

Step Four: Identify the IO Assets, Derive the IO Sub-tasks, and Prepare the Candidate Master IO Target List

FORM 19: Identify the IO Asset, derive the IO Sub-tasks, and prepare the candidate IO Master Target List. **Identify the specific IO Asset most appropriate for achieving the Effects desired on the selected critical and vulnerable targets; evaluate to select the one most capable of producing the desired Effect on the target.** There may be a variety of Assets capable of producing the Effect desired on a given target; there may also be only one or two. In this step, planners will need to consider not only the technical ability of an IO Asset to produce the Effect desired, but also whether or not that IO Asset is:

- Apportioned
- Assigned
- Allocated
- Deployed
- In-commission (not battle-damaged or destroyed)
- Otherwise available

Planners also must consider the adequacy and availability of allied and special IO Assets to accomplish the desired Effect on the target selected. Planners can think of IO in terms of their ability to cause a broad range of Effects or very specific Effects. For example, planners may want to begin their search for the most appropriate IO Asset to apply by grouping Assets in categories by IO specialty, i.e., Electronic Warfare Assets, Destruction Assets, Deception Assets, Computer Network Attack Assets, and etc. Then, within these categories, planners can search for Assets that will induce the desired Effect, i.e., Deny, Destroy, Degrade, Disrupt, Influence, Mislead or any other Effect desired (some examples of other potential effects are corrupt, sever, confuse, and so forth). Planners may also choose to further

categorize their search by Assets available from each component. Some factors to consider when evaluating IO Assets to select the one best capable of achieving the Effect desired include the following:

Availability – How readily can the Assets be made available to use against the target;

Duration – What is the duration of the Effect caused by the IO Assets;

Delivery Error – Can the IO Assets be delivered to the target within acceptable accuracy limits;

Probability of Effect – What is the probability that the Effect will be achieved; and

Asset Reliability – How reliable is the IO Asset to be applied?

Once the best Asset is selected to cause the Effect desired, write the Target, Effect, and Asset on the form.

FORM 19A: Identify the IO Asset, derive the IO Sub-tasks, and prepare the candidate IO Master Target List. **Identify the specific IO Asset most appropriate for achieving the Effects desired on the selected critical and vulnerable targets; evaluate to select the one most capable of producing the desired Effect on the target.** *This is an optional step.* These forms allow the planner to refine the evaluations made in the previous step by allowing for weighted mathematical analysis to derive the best IO Asset to apply to induce the Effect desired. The criteria to be employed are:

- Availability
- Probability of Achieving Effect
- Duration
- Weapon Reliability
- Delivery Error

AVAILABILITY = Availability of an IO Asset for applying an Effect to a Target during a specific time frame.

RATING SYSTEM for Availability

LOW = IO Asset will be in limited availability, or will not be available.

MEDIUM = IO Asset will be available to apply the desired Effect against the specified Target.

HIGH = IO Asset is available. Availability of the Asset may extend beyond the required time frame and/or is available in more than sufficient supply.

PROBABILITY OF EFFECT = Degree to which IO Asset can induce desired Effect.

RATING SYSTEM for Probability of Effect

LOW = probability of achieving Effect is low.

MEDIUM = probability of achieving Effect is moderate.

HIGH = probability of achieving Effect is high.

NOTE: Probability of achieving Effect Measures of Effectiveness (MOEs) may be available in engineering tools off-line. These MOEs may facilitate the evaluation of IO Assets.

DURATION = Degree to which the duration of damage caused by the IO Asset meets mission requirements

RATING SYSTEM for Duration

LOW = duration does not meet mission requirements

MEDIUM = duration meets mission requirements

HIGH = duration exceeds mission requirements

ASSET RELIABILITY = Degree to which the IO Asset is reliable against the type of target

RATING SYSTEM for Asset Reliability

LOW = reliability is low

MEDIUM = reliability is moderate

HIGH = reliability is high

DELIVERY ERROR = Probability and percentage of error associated with IO Asset delivery

RATING SYSTEM for Delivery Error

LOW = error rate is high

MEDIUM = error rate is moderate

HIGH = Error rate is low

Evaluate the list of IO Assets against the provided criteria (Default scheme is: Availability, Probability of Effect, Duration, Asset Reliability and Delivery Error are weighted at .20 each; the value for Low = .2; Medium = .5; and High = .8) to determine the best IO Asset to apply to the target to achieve the desired Effect. Use the weighting scheme provided to make the calculations indicated on the form to arrive at a numerical total. The higher the total, the greater the potential for the IO Asset is to achieve the desired Effect.

FORM 20: Identify the IO Asset, derive the IO Sub-tasks, and prepare the candidate IO Master Target list. **Evaluate the selected Asset-Target Pairs in light of Cost-Risk-Benefit criteria and select the final Asset-Target pairs.** The results of accomplishing the previous steps yielded a listing of:

- Hardware, software, wetware or data targets most critical to the success of an adversary's Function, and most vulnerable to friendly IO Assets
- A reconfirmation and de-confliction of Effects desired on the targets selected
- The selection of an IO Asset best able to cause the Effect desired

In this step, the planner will evaluate the list of targets and Assets to select, based on a cost-risk-benefit evaluation, the best ones to attack.

Factors that can be considered when conducting the cost-risk-benefit evaluation include the following:

Cost - in terms of *number, value, and consequences*

Risk - in terms of *probability of failure, consequences of failure, capability compromise, and collateral damage*

Benefit - in terms of *impact, probability of success, confidence, political consequence, cost to reconstitute*

After completing the evaluation, select the final Asset-Target pairs and write them on the form.

FORMS 20A and 20B: Identify the IO Asset, derive the IO Sub-tasks, and prepare the candidate IO Master Target list. **Evaluate the selected Asset-Target Pairs in light of Cost-Risk-Benefit criteria and select the final Asset-Target pairs.** *This is an optional step.* In this step, there are two forms: one for the cost, risk, and benefit calculation, and one to make the final calculation to derive the best Asset-Target pairs. These forms allow the planner to refine the evaluations made in the previous step by using weighted mathematical analysis to derive the best Asset-Target pairs. The criteria (Default scheme is: Cost, Risk, and Benefit are weighted at .33 each; the value for Low = .2; Medium = .5; and High = .8) to be employed are:

- Cost
- Risk
- Benefit

COST = Aggregate costs of using the IO Asset being evaluated on the target in question. Cost has three sub-components that can be assessed when making the calculation:

CONSEQUENCES = Political consequences of weapon use/target choice

NUMBER = Number of weapons required to accomplish mission

VALUE = Monetary value/cost of weapon

RATING SYSTEM for Cost

LOW = Aggregate costs of IO weapon employment on this target are low

MEDIUM = Aggregate costs of IO weapon employment on this target are medium

HIGH = Aggregate costs of IO weapon employment on this target are high

RISK = Aggregate risk incurred when using this IO weapon on this target. Risk has four components that can be assessed when making this calculation:

PROBABILITY OF FAILURE = Probability that the attempt to employ this IO weapon on this target will fail to produce the Effect desired

CONSEQUENCES OF FAILURE = Consequences if the attempt to use this IO Asset on this target fails

CAPABILITY COMPROMISE = Risk of compromising sensitive capabilities (technical prowess, delivery Asset, intelligence sources, etc.) when using this IO Asset against this target

COLLATERAL DAMAGE = Potential for collateral damage if this IO Asset is used on this target

RATING SYSTEM for Risk

LOW = Aggregate risk of employing this IO weapon on this target is low

MEDIUM = Aggregate risk of employing this IO weapon on this target is medium

HIGH = Aggregate risk of employing this IO weapon on this target is high

BENEFIT = Aggregate benefit accruing when using this IO Asset on this target. Benefit has five components that can be assessed when making this calculation.

PROBABILITY OF SUCCESS = Probability that the attempt to employ this IO Asset on this target will succeed in causing the Effect desired

POLITICAL ACCEPTABILITY = Political acceptability of using this IO Asset on this target

CONFIDENCE = Confidence that use of this IO Asset on this target will meet the friendly operational requirements and objectives

IMPACT = Impact on opposition of use of this IO Asset on this target

RECONSTITUTION = Cost to opposition of reconstitution if this IO Asset is applied to this target

RATING SYSTEM for Benefit

LOW = Aggregate benefit of employing this IO weapon on this target is low

MEDIUM = Aggregate benefit of employing this IO weapon on this target is medium

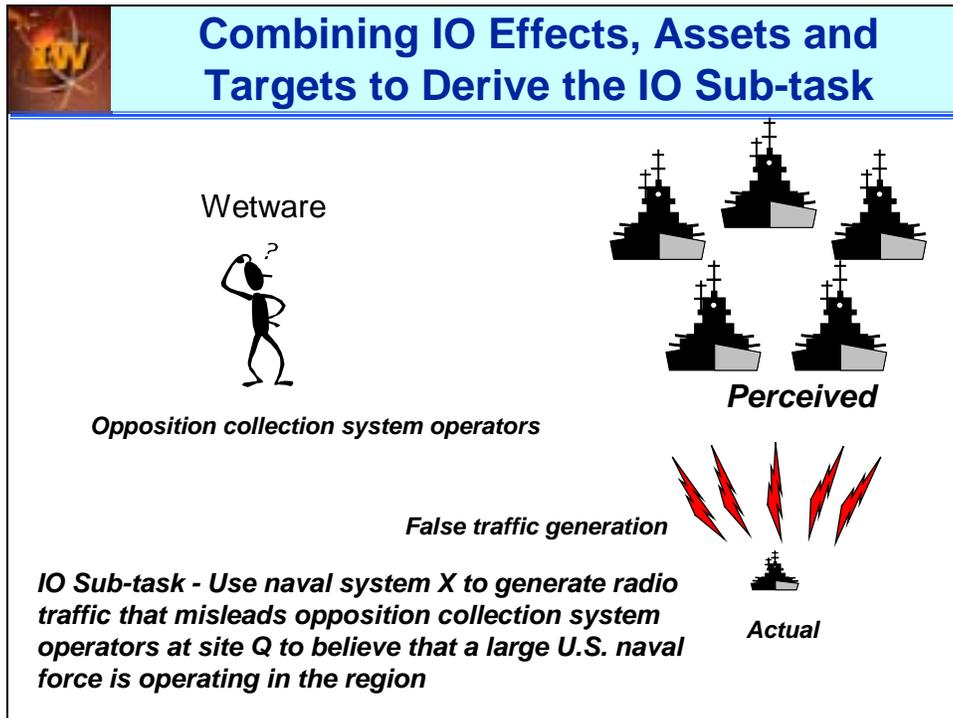
HIGH = Aggregate benefit of employing this IO weapon on this target is high

After deriving the numerical values for cost, risk and benefit, use the formula on FORM 20B to determine overall target value. This value can be a principal consideration when assembling a prioritized list of targeting options.

FORM 21: Identify the IO Asset, derive the IO Sub-tasks, and prepare the candidate IO Target List; **Derive and write IO Sub-tasks.** The IO Sub-task statement is intended to be a clear statement of what is to occur. The IO Sub-task should include the following:

- The IO Objective
- The Effect to be induced
- The Function to be affected
- The specific Target to be affected
- The specific IO Asset to be applied

The Chart below illustrates one such completed IO Sub-task:



FORM 22: Identify the IO Asset, derive the IO Sub-tasks, and prepare the candidate Master IO Target List. **Prepare the candidate Master IO Target List.** On this form, the candidate Master IO Target list is assembled. On the form, list the target name; the Basic Encyclopedia number if assigned; the category code; the coordinates/location; and the IO Asset to be applied. Gather the information specified and write the information on the form.

Step Five: Conduct Equity Review

FORM 23: Conduct Equity Review. Review IO Sub-tasks in light of appropriate checklists to ensure various equities are properly considered. The review of equities is the final step in the Joint IO Attack Planning Process. On this form, the various IO Sub-tasks are reviewed to ensure that they are checked against other factors that may bear on the attack of IO targets. These other factors include the following.

1. **Operational gain versus intelligence loss** – This dilemma is well known to most planners. Another way of stating the issue is “Do we shoot (or watch), or listen?” Though processes exist for conducting the reviews of the equities involved among the interested parties in both the intelligence and operational communities, the group of those involved usually grows larger when IO are involved. This is because the SECDEF is the ultimate IO “warfighter” and equity review may well include review at the SECDEF level for not only this category, but others as well.
2. **Joint Restricted Frequency Lists** – The Joint Spectrum Center is principally responsible for the construction of these lists. The J6 will also be involved, as well as the J2. The IO planner is ensuring here that IO will not impact friendly attack or defensive communications or other operations negatively.
3. **Security Compromise** – This factor may become crucial if sensitive, perishable, high cost technologies are to be employed in the hope of achieving a specific war-fighting goal. The question here is “does the expected operational outcome justify the potential exposure of high cost, technically perishable technologies?” Alternatively, this factor could include an assessment of the risk of exposing IO methods and techniques that are or have been extremely effective, and whose utility may be completely neutralized if exposed.
4. **No Strike** – This factor is designed to search for targets that, if struck with any given IO Asset, would cause an unacceptable level of unintended damage to another Function or structure. The simplest example is one where an IO target is next to a hospital, school, or other non-combatant structure. Another example may be where a given IO Asset is used to affect an adversary’s joint military-civil-commercial communications network that friendly forces may wish to preserve for other purposes.
5. **Service** – Service equities can be considered when finalizing IO plans. The assigning of destroy Effects on adversary air defense systems to one Service or Component day after day, with concomitant probability of recurring high casualty rates, is sufficient to warrant close review of equities.
6. Once the equities are reviewed and adjusted, the candidate Master IO target list will be forwarded for de-confliction/integration with the Air Tasking order and other attack orders. Once de-conflicted and integrated, it becomes the Master IO Target List.

Class Slides

The following slides illustrate the key points of this chapter and are used as part of the Joint IO Planning Course class that covers IO planning.



JIOPP Background

- **Joint IO Planning Process (JIOPP) developed in response to JCS / Unified Command J3 need for a formal, standardized, integrated IO planning process common to all planning echelons**
 - **Clearly show how IO helps accomplish Combatant Commander objectives**
- **Planners do the thinking, computers “keep the books” and allow access to tools**
- **Provides a needed, repeatable, verifiable process**
- **Development process has highlighted need for more and different products to support IO planning**

The JIOC has developed two formalized planning processes for IO. Combined, these processes are called the Joint IO Planning Process (JIOPP). The JIOPP has distinct offensive and defensive modules as shown here.

The JIODPP is a fully developed and validated process that is used by JIOC CC support teams to plan defensive IO for the Unified Commanders.

The JIOAPP is still under evaluation, but has already proven its value in both exercise and operational use.

The ultimate goal of the JIOC is to fully integrate both processes into the Global Command and Control System software suite.



JIOPP Background

- There are two JIOPP planning modules -- attack and defense
 - Joint IO Attack Planning Process (JIOAPP) has been used to conduct exercise and operational IO planning
 - Computer application that implements JIOAPP – called IO Navigator (ION) – in use since January 2000
 - Improved ION Release 2 operational 30 April 2001
 - Joint IO Defensive Planning Process (JIODPP) has completed IO community review / validation; development of JIODPP portion of ION started August 2001
 - Integration of both modules in progress
- Risk management-based approach incorporates Combatant Commander objectives and values, accounts for adversary capabilities, and facilitates cost-risk-benefit analysis among D-IO methods / techniques
- JIOC will continue refining JIOPP based upon ongoing operational employment of the process
- Long-term goal – integrate JIOPP into GCCS



Why a Special Planning Process for IO?

SECDEF and
CC
Objectives

CC IO Cell

Standard
Planning
Process

Unless there is a repeatable process, an IO cell must reinvent the approach it uses to approach the new problems and issues of each new contingency.

The JIOPP process is designed to help make IO planning easier while maximizing flexibility and creativity.

While each step of the process should be performed, the process may be done to whatever degree of detail is desired based upon the available time for planning.

IO Objective

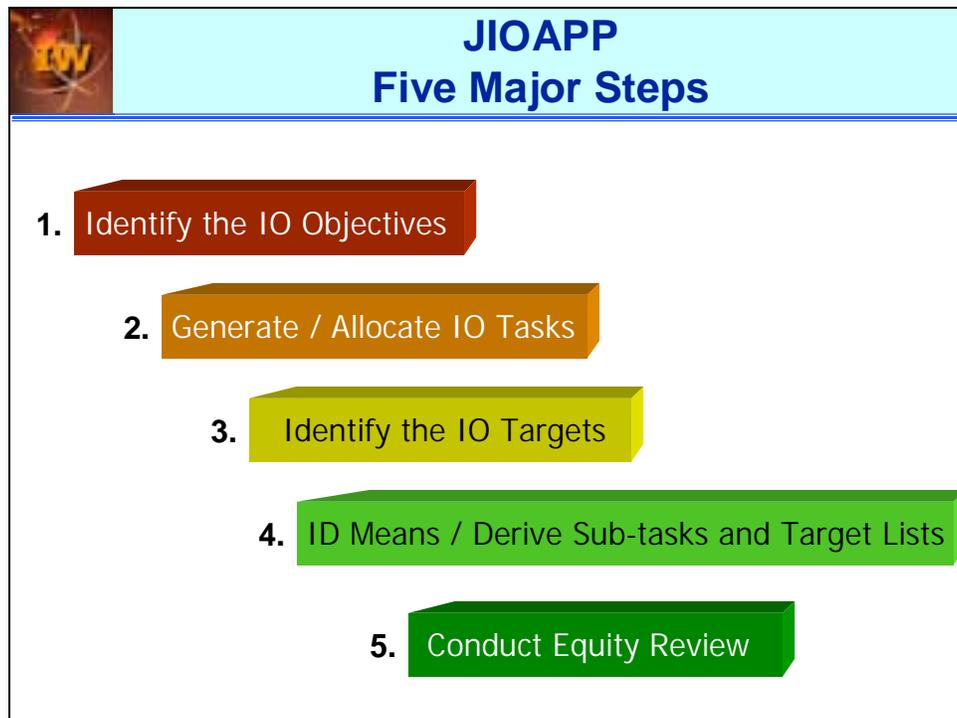
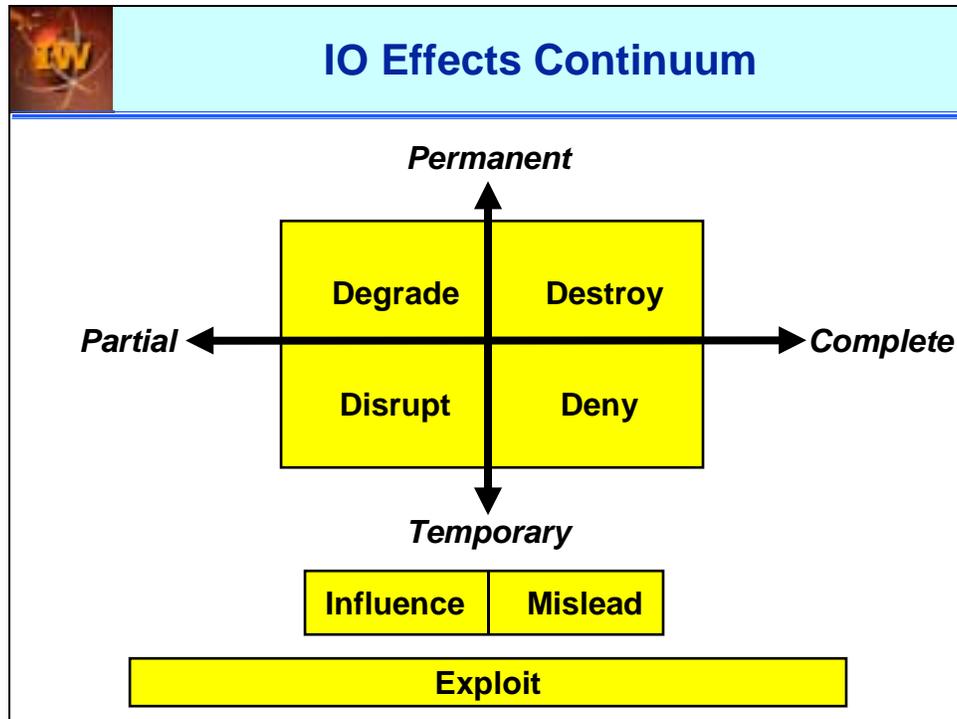
IO Task

IO Sub-task

IO Action

Plan Elements

So why did we develop a special planning process for IO? The answer is really simple. It was necessary to give IO planners a method that would allow them to approach each new problem in a standard manner without hindering their flexibility or creativity. The JIODPP was the answer. The added benefit of having a standardized process was that it lends itself to being automated. The JIOAPP has been incorporated into the JIOC's IO planning software called the IO Navigator (ION). The JIODPP module for ION is still under development.



The equity review needs to be done at the CC level, and then again down at the JF/component level.



JIOAPP

Attack Module Core Process

SECDEF Mission

CC Objectives – What must be done to accomplish NCA mission?

Specified, Implied, Subsidiary Tasks – (QA) How can IO help?

IO Objectives – What will we do from an IO perspective?

Activities and Functions – (QA) Where will we focus our efforts? Intelligence / Tools
(e.g. SIAM)

General Effects and Elements – How will we shape the info Environment?

CC IO Tasks – Focused on Centers of Gravity

JFC High Value IO Targets – (QA) What are best Targets in COGs? Intelligence & Engineering Tools
(DIODE / ADVERSARY)

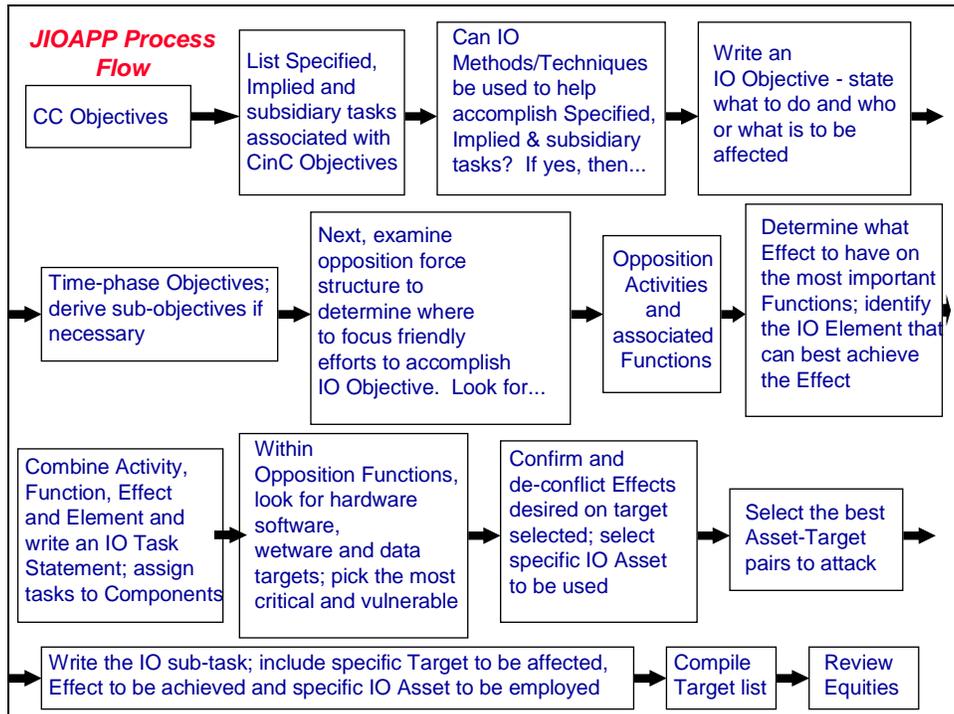
JTF Specific Effects and Assets – (QA) What are best Assets to induce Effect desired? Weaponering and Engineering
Tools (CNMTE)

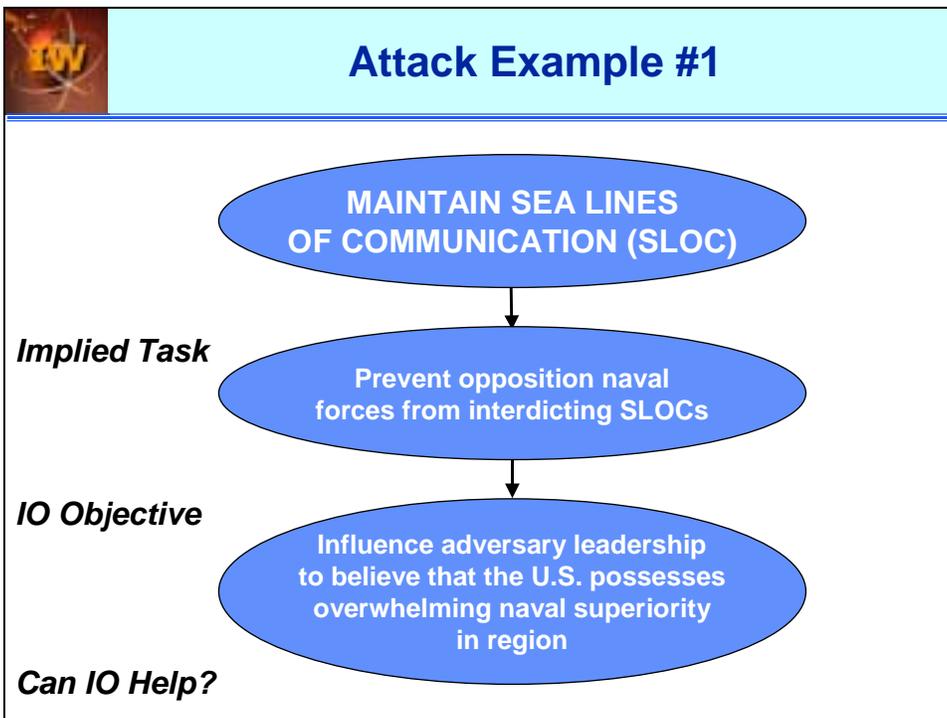
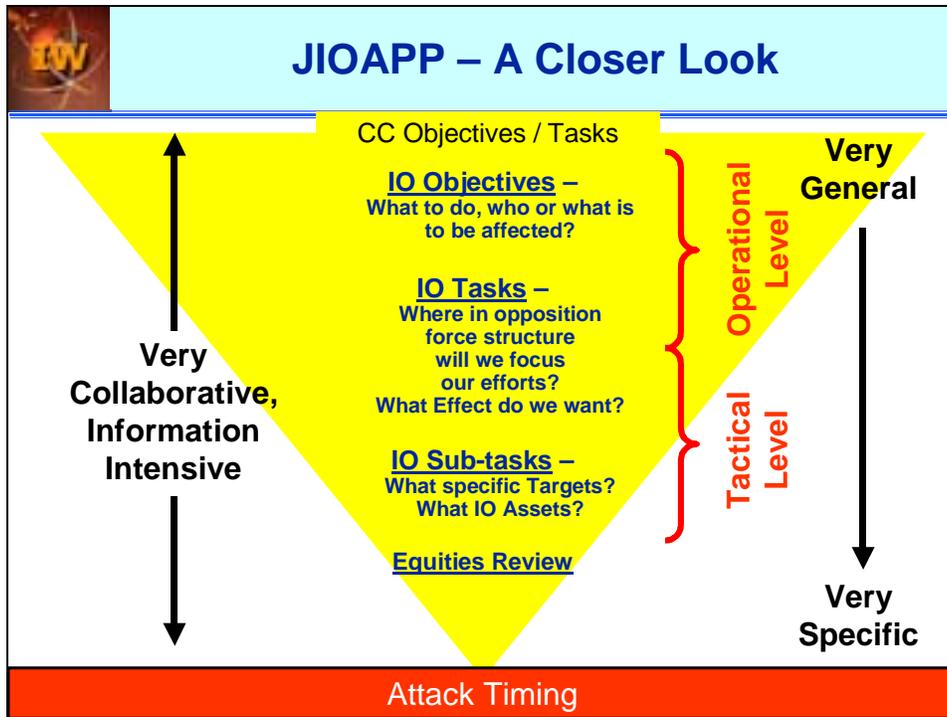
High Payoff IO Targets – (QA) What are best combos of Target / Asset? Decision Tools

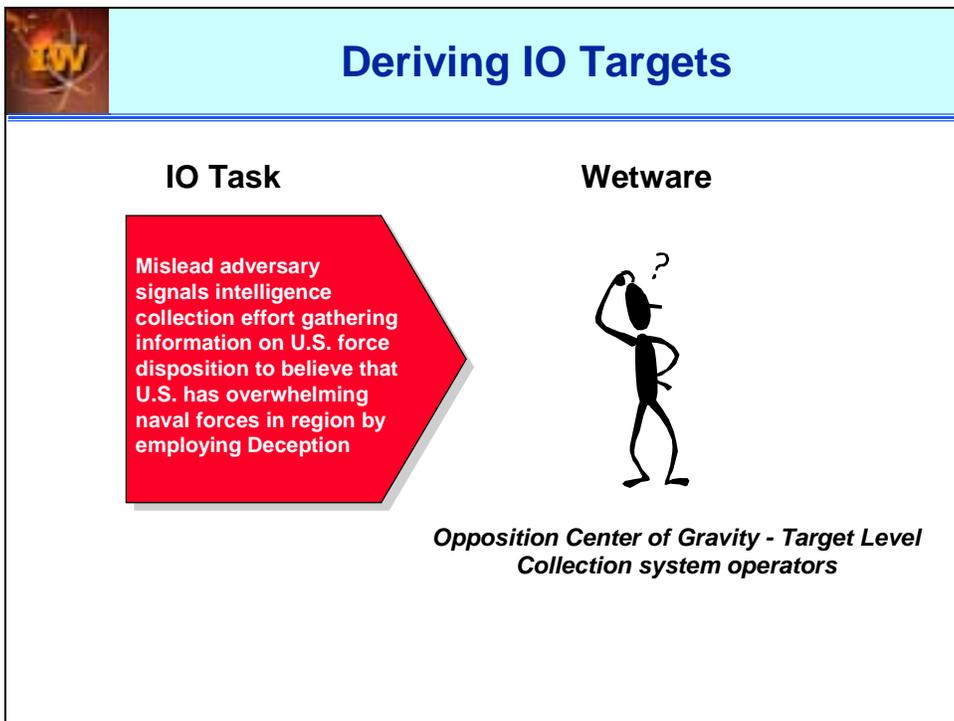
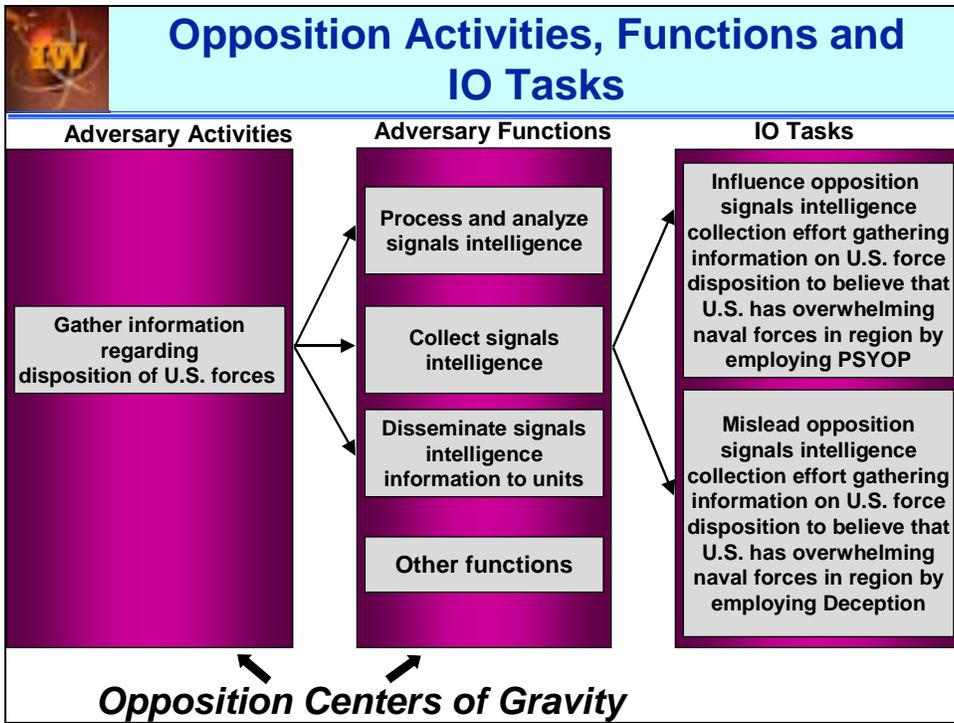
IO Sub-tasks – Plain language statement of purpose

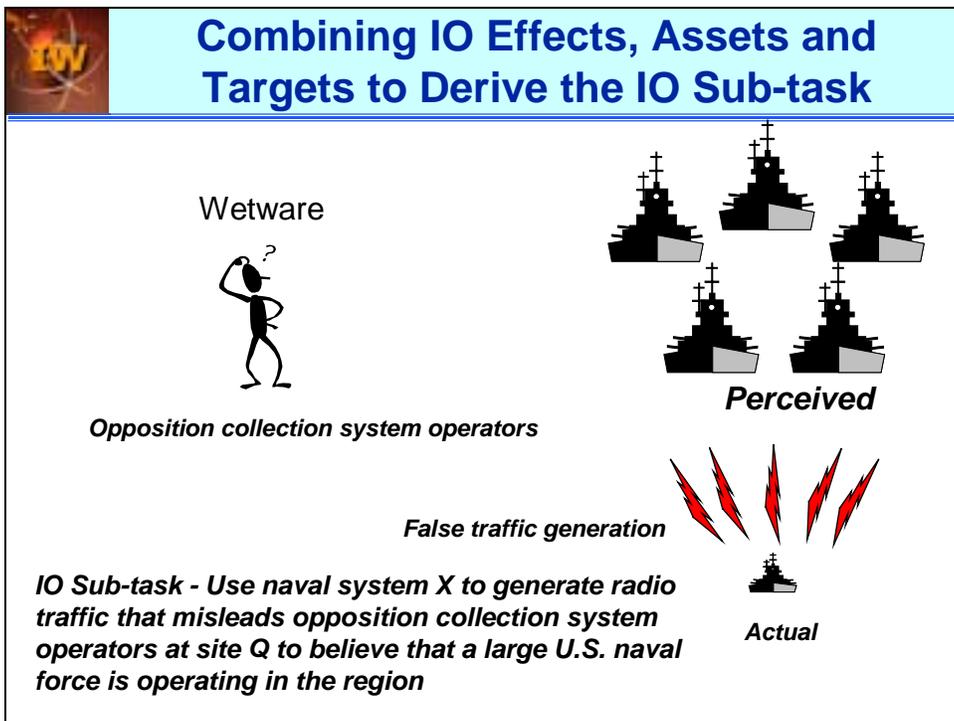
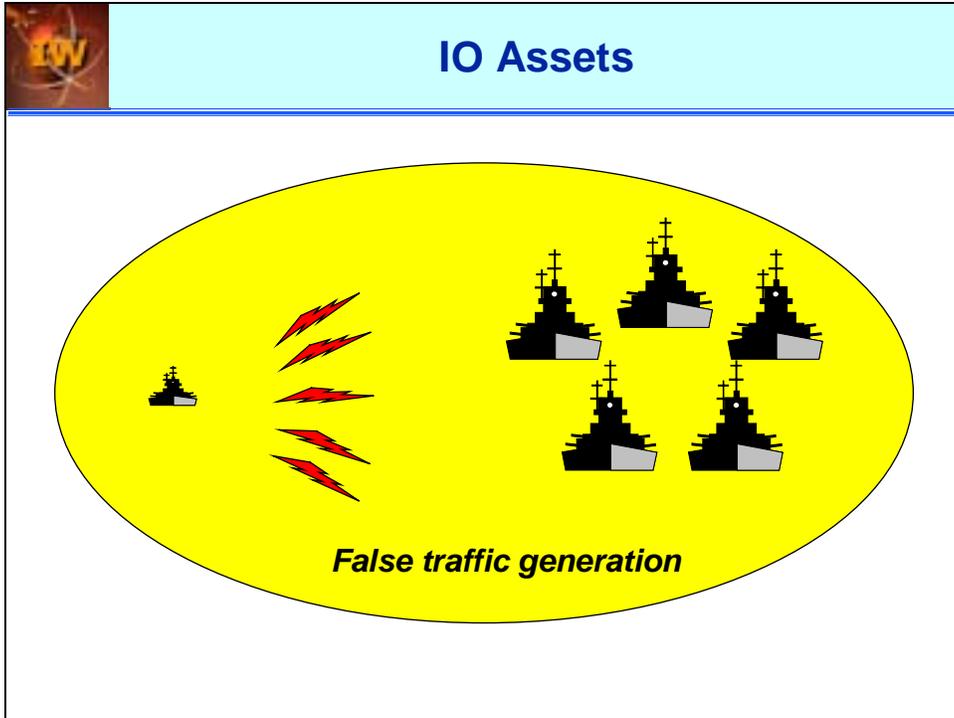
Actions – Coordinated Targets with Timing

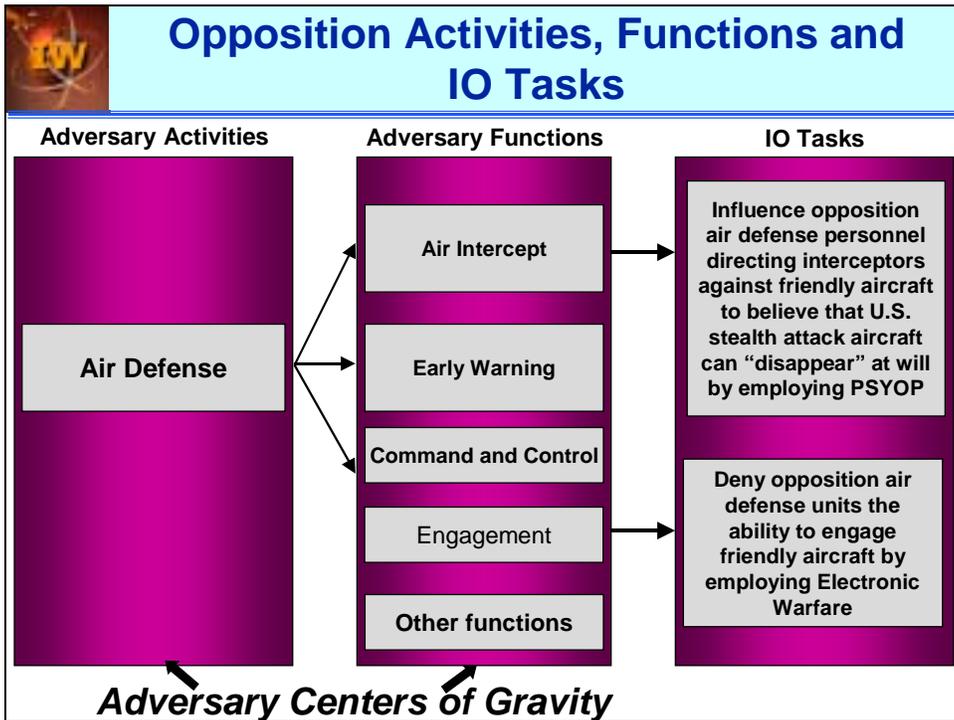
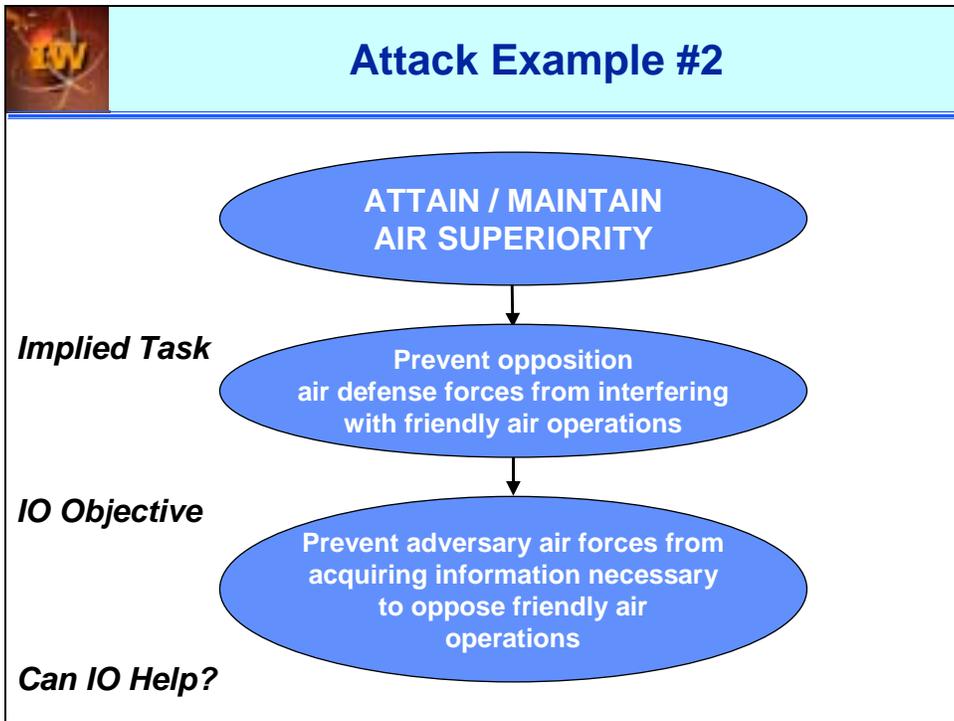
QA = Quantitative Analysis













ID Assets and Allocate to Targets

- Which Assets best accomplish the Effect we wish to have on target?
- Which Assets . . .
 - AppORTioned?
 - Available?
 - Deployed?
 - Special?
 - Allied?
- Synergistic Assets?
- Relationship to defensive actions?

Conduct Equity Review

	Ops gain / Intel loss	JRFL	Security Compromise	No strike	Service
Sub-task 1	✓	✓			
Sub-task 2	X	✓	X		
Sub-task 3					
Sub-task 4					
Sub-task 5					

Review IO Sub-tasks in light of appropriate checklists to ensure various equities are properly considered

This page intentionally left blank

Chapter VI – Joint Information Operations Defensive Planning Process

The Joint Forces Staff College would like to thank the Joint Information Operations Center for providing the materials for this chapter. Slides illustrating main points start at page VI-18.

Introduction

Much attention has been given in recent years to planning the technical aspects of Defensive IO, namely Information Assurance (IA) and Computer Network Defense (CND). The responsibility for these functions is often given to a CC's J6. A look at the recent literature on defensive IO leaves one with the distinct impression that Defensive IO equals IA and CND. Too little has been written on planning full-spectrum defensive IO. This chapter focuses primarily on the non-technical disciplines involved in deliberate, defensive IO planning. The methodology discussed is the Joint IO Defensive Planning Process (JIODPP). Personnel of the Joint Information Operations Center (JIOC) in San Antonio, Texas developed the JIODPP.

The JIODPP discussed in this chapter is a five-step methodology for conducting Defensive IO Planning. The JIODPP is part of the Joint IO Planning Process (JIOPP). The JIOPP includes, in addition to the JIODPP, the Joint IO Attack Planning Process (JIOAPP), the attack planning complement to the JIODPP. The JIOPP provides a logical, structured method for integrating Information Operations (IO) planning into the Joint Planning Process.

The JIODPP facilitates planning at two levels – that conducted by the Unified Commands, as well as the subordinate Component Commands. Unified Command defensive IO planning usually has as its objective the construction of detailed defensive IO task statements that are provided to the Components for further planning. Component-level planning strives to determine the optimum balance among the Combatant Commander's Objectives, assets to be protected and D-IO Means. Since the defensive IO planning process is information-intensive, it can also be highly collaborative in nature. Thus, information and expertise from sources and staffs outside the CC's IO Planning Cell will be needed to apply the JIODPP most effectively. Further, the responsibility for conducting contingency planning is shared among the Unified Commands and their Components, the Joint Chiefs of Staff, and Department of Defense Agencies and Centers. The CINCs of the various Unified Commands bear the primary responsibility for executing those plans and therefore have the lead in plan development. The JIOC assists the Unified Command staffs in developing IO concepts, integrating these into contingency plans, and assisting in their execution.

The guidelines presented above regarding the roles of and boundaries between Unified Command, Component, and other planners may regularly shift. Planners at all levels should not hesitate to contact persons or staffs (or consult on-line sources) that can provide or acquire needed information.

The following information will assist you in using the JIODPP "paper process" to conduct defensive IO planning in support of CC objectives. The purpose of each form will be explained and amplifying information provided as needed to help you complete the form. Because each planning situation is different, more forms than are provided in the initial package may be needed to complete a particular step. If more forms are needed, they can be easily acquired.

The Five Steps of the Joint Information Operations Defensive Planning Process

The five major steps of the JIODPP are listed below. There are a series of sub-steps associated with each of the major steps. The major steps and sub-steps are as follows.

1. Identify the Defensive IO (D-IO) Objectives

- a. Import/write CC objectives
- b. Identify Specified, Implied and subsidiary tasks associated with the CC objectives
- c. Pair Specified, Implied and subsidiary tasks with defensive IO methods and techniques that may help accomplish the tasks
- d. Evaluate the ability of defensive IO methods and techniques to help accomplish the Specified, Implied and subsidiary tasks
- e. Write a defensive IO Objectives statement for tasks selected; establish phasing of defensive IO Objectives; derive and phase defensive IO Sub-objectives as required

2. Generate the D-IO Tasks

- a. For each conflict phase, write the friendly Activity that must be protected to satisfy the defensive IO Objective
- b. For each activity, identify the functions that most contribute to the friendly activity
 - (1) Evaluate the functions to determine their importance to the activity's success; select the most important functions
- c. Identify the Effects an opponent may attempt to induce on the selected functions
- d. Review the range of Effects possible on the selected functions
- e. Identify the Defensive IO Means Sets most suitable to protect against the Effects possible
- f. Write and establish phasing for a defensive IO Task Statement based on: friendly activity and function to be protected, Effect to be defeated, and defensive IO Means to be applied to achieve protection from the Effect
- g. Determine which Component has the best capability to accomplish the IO Task/Sub-task; distribute the IO task to the Component(s)

3. Identify Assets to be protected and conduct Risk Analysis

- a. Identify the IO assets – characterized as hardware, software, wetware or data assets--that must be protected to defeat/prevent the Effect an opponent is attempting to induce on the friendly function
- b. Confirm or refine Effects possible on assets to be protected
- c. Evaluate and select the hardware, software, wetware and data assets associated with the function to identify the ones most critical to the function's success; evaluate the assets further to identify the ones most vulnerable to enemy attack
 - (1) Evaluate the Assets according to the criteria for impact of loss (critical)
 - (2) Plot the impact of loss value for the evaluated asset on the chart
 - (3) Evaluate the assets according to the criteria for probability of loss (vulnerable)
 - (4) Plot the probability of loss value for the evaluated asset on the chart
 - (5) Plot the combined value for the evaluated asset on the chart

4. Select Protection Measures and derive the Defensive IO Sub-tasks

- a. Identify the specific defensive IO Means most appropriate for diminishing the risk posed by adversary-induced Effects on the selected critical and vulnerable IO assets
- b. Evaluate to select those most capable of diminishing the adversary-induced Effect on the Asset
 - (1) Evaluate the D-IO Means according to the criteria for diminishing impact of loss of a critical Asset

- (2) Plot the reduction in Impact of Asset Loss conferred by the Defensive IO Means
- (3) Evaluate the Defensive IO Means according to the criteria for diminishing probability of loss of a vulnerable Asset
- (4) Plot the reduction in probability of Asset loss conferred by the Defensive IO Means
- (5) Plot the overall reduction in risk to the Asset conferred by the Defensive IO Means
- c. Select Defensive IO Means-Asset combinations to minimize risk of adversary-induced Effect
- d. Identify costs associated with the selected Means-Asset combinations in light of cost criteria
- e. Select the final Means-Asset combinations by calculating protection value according to the formula
- f. Derive and write the Defensive IO Sub-tasks

5. Prepare the Master Protection List and conduct Equity Review

- a. Prepare candidate Defensive IO Master Protection List
- b. Review Defensive IO Sub-tasks in light of appropriate checklists to ensure various equities are properly considered

FORMS – GENERAL INSTRUCTIONS: To facilitate planners' ability to orient themselves when using this "paper process," the bottom of the form will display a statement succinctly stating what information is to be recorded on the form. The top of each form will display the major step of the JIODPP to which the form pertains.

Step One: Identify the Defensive Information Operations Objectives

FORM 1. Identify the Defensive IO Objectives. **Write the CC Objectives.** The purpose of this form is to record the CC objectives. In many instances, the IO planning cell will be **provided** the CC Objectives. In other cases, the IO Planning Cell may be involved in **deriving** the CC Objectives. Further, CC defensive objectives may be identified as a consequence of CC attack planning, and may be **"imported"** from the IO attack-planning module. The exact way by which CC Objectives will be determined will probably vary by CC staff and conflict scenario. The most important point here is to capture and record **all** CC Objectives.

FORM 2. Identify the Defensive IO Objectives. **Identify Specified, Implied and subsidiary tasks associated with the CC Objectives.** The purpose of this form is to record the Specified, Implied and subsidiary tasks. Upon receipt of a mission, the commander (in concert with his staff) begins his mission analysis by asking himself specific questions about higher headquarters or SECDEF purpose, intent, the area of operations, available assets, constraints, restrictions, risk, and time. The commander will subsequently disseminate the results of his analysis in his restated mission description, objectives, and concept of operations. The staff continues the mission analysis by asking additional questions, the most important of which is:

"What tasks must the command perform to accomplish the assigned mission successfully?"

To answer this question, extract (with no consideration of IO) specified, implied or subsidiary tasks from the commander's objectives, concept of operations, mission statement and rules of engagement.

SPECIFIED TASKS are those tasks the commander spells out in the mission description, his operational objectives, his concept of operations and other guidance. They are what the commander wants accomplished.

IMPLIED TASKS are those additional major tasks that are necessary to accomplish the mission, but which are not specifically spelled out in the commander's guidance. They should not be routine, standing operating procedure type tasks, or inherent responsibilities of the commander; e.g. providing flank

protection for his own unit. Limit the implied tasks to major tasks that are "essential" to the accomplishment of the mission. Use available task lists (Uniform Joint Task List, Mission Essential Task List, etc.) to assist in this process.

SUBSIDIARY TASKS are any other tasks that could be viewed as supporting the mission.

FORM 3. Identify the Defensive IO Objectives. **Pair Specified, Implied and subsidiary tasks with Defensive IO Methods and Techniques that may help accomplish the tasks; select the ones that will best help accomplish the tasks.** In this step, first examine the specified, implied and subsidiary tasks to determine what role Defensive IO may be able to play in accomplishing the tasks. Ask: can the Defensive IO methods and techniques listed on the form help accomplish the tasks? Pair specified, implied and subsidiary tasks with the IO Method or Technique that can best help accomplish the task, and enter these on the form along with the task.

FORM 4. Identify the Defensive IO Objectives. **Evaluate the ability of Defensive IO Methods and Techniques to help accomplish the Specified, Implied and subsidiary tasks.** The next step is to evaluate how well the specified/implied/subsidiary tasks can be accomplished using Defensive IO methods and techniques. To do this, assess the ability of Defensive IO Methods and Techniques to help accomplish the designated task according to these criteria: **Capability, Feasibility, and Constraints.**

CAPABILITY = Degree to which Defensive IO has the capability to accomplish or support the objective. Capability has two sub-components that can be considered when making the assessment. These are:

EFFICIENCY = Efficiency of D-IO in accomplishing the mission

SUCCESS = Probability of success associated with D-IO in achieving the objective

RATING SYSTEM for Capability

LOW = D-IO cannot accomplish or support accomplishment of the objective.

MEDIUM = D-IO may be able to accomplish or support accomplishment of the objective.

HIGH = D-IO can definitely accomplish or support accomplishment of the objective.

CONSTRAINTS = Degree to which constraints favor or disfavor use of D-IO. Constraints have three sub-components that can be considered when making the assessment. These are:

POLITICAL = Degree to which political constraints favor or disfavor use of D-IO

RULES OF ENGAGEMENT = Degree to which ROE favor or disfavor use of D-IO

CULTURAL = Degree to which cultural (religion, etc.) constraints favor or disfavor use of D-IO

RATING SYSTEM for Constraints

LOW = constraints preclude the use of D-IO.

MEDIUM = constraints permit the use of D-IO.

HIGH = constraints cause preference for use of D-IO.

Evaluate the list of specified, implied and subsidiary tasks against the provided criteria to determine the applicability of D-IO to successful task accomplishment. Use the weighting scheme provided (Default scheme is: Capability, Feasibility and Constraints are weighted at .33 each; the value for Low = .2; Medium = .5; and High = .8) to make the calculations indicated on the form to arrive at a numerical total; the higher the total, the greater the potential contribution of D-IO to accomplishing the task.

FEASIBILITY = Degree to which D-IO is a feasible means for accomplishing or supporting the objective. Feasibility has three sub-components that can be considered when making the assessment. These are:

TECHNICAL = Technical feasibility of D-IO method/technique to protect against potential opposition-induced Effects

RESOURCES = Degree to which resources are available to implement D-IO capabilities

TIME = Degree to which sufficient time exists to implement and achieve D-IO results

RATING SYSTEM for Feasibility

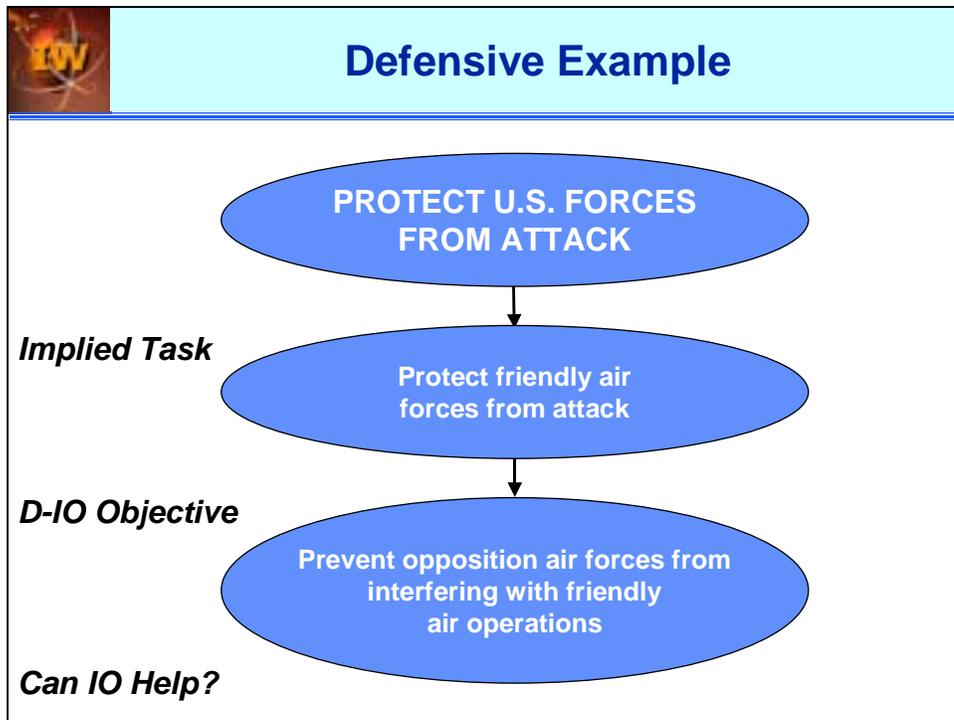
LOW = using D-IO is NOT feasible.

MEDIUM = using D-IO may be feasible.

HIGH = using D-IO is feasible.

FORM 5. Identify the Defensive IO Objectives. **Write a D-IO Objective statement for Tasks selected.** Enter the Defensive IO Objective Statement on the form. The Defensive IO Objective statement can include the general class of assets or audience to be protected, and may state what the desired outcome may be. An example is shown in the following chart:

SAMPLE DEFENSIVE IO OBJECTIVE DERIVATION



FORM 6. Identify the IO Objectives. **Establish time phasing of Defensive IO Objectives.** On this form, assign the accomplishing of Defensive IO Objectives to the desired phase of the campaign. Assign start and end dates for the Defensive IO Objective and reference the phasing in relation to D-Day. The opportunity will be provided to review and refine the phasing data throughout the planning process.

FORM 7. Identify the IO Objectives. **Derive and write Defensive IO Sub-objectives as necessary.**

NOTE: *The derivation of Defensive IO Sub-objectives is optional.* Sometimes, the further breakdown of Defensive IO Objectives into sub-objectives is warranted to identify more specifically protection desired or

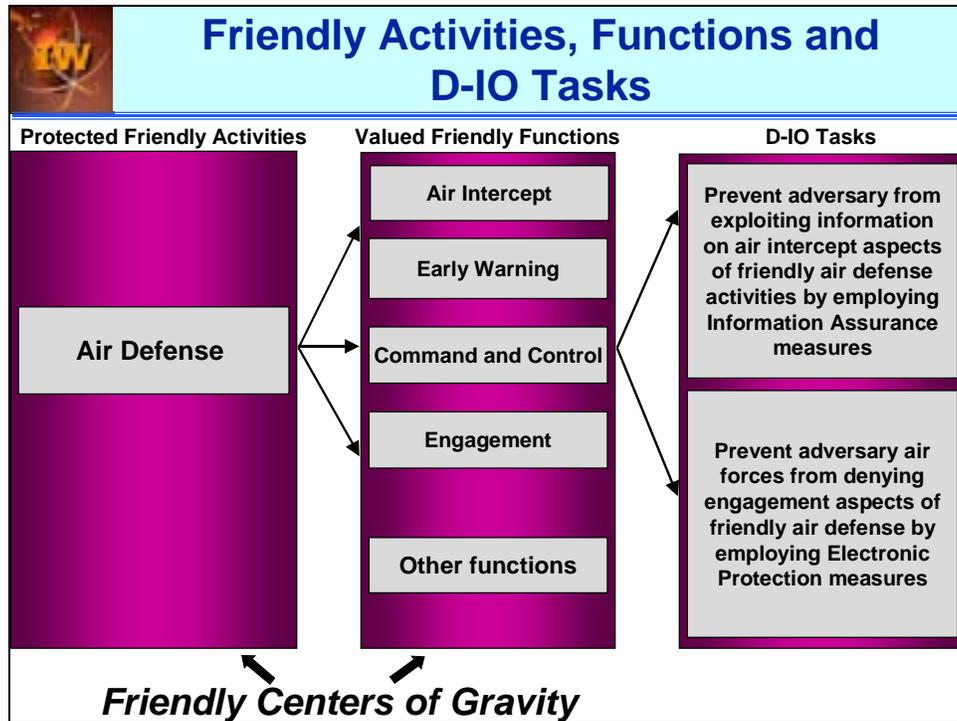
to further delineate classes of assets to be protected. Continuing the example given in the chart for Form 5, a defensive IO Sub-objective could perhaps specify distinct classes of assets to protect within the friendly air operations structure – the air intelligence leadership or the air defense leadership, for example – or a specific air defense sector. The sub-objective derivation would consider the Defensive IO Methods and Techniques available and the friendly centers of gravity to be protected. Any Defensive IO Sub-objectives derived should be phased.

Step Two: Generate the Defensive Information Operations Tasks

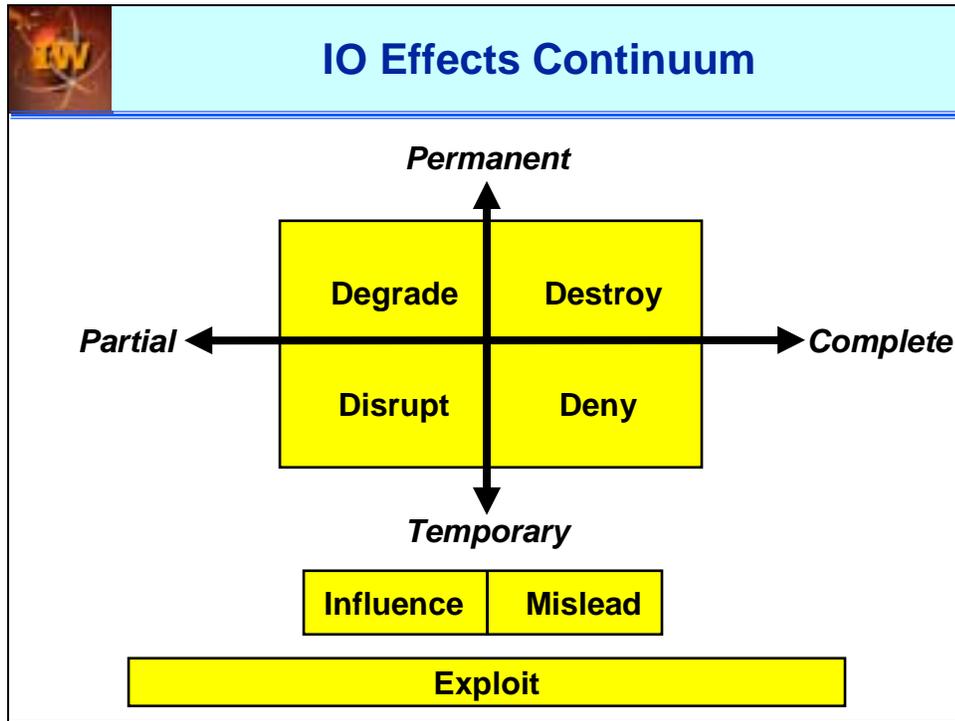
FORM 8. Generate the Defensive IO Tasks. **For each conflict phase, write the Friendly Activity that must be protected to satisfy the Defensive IO Objective.**

On this form, list friendly **Activities** to be protected by Defensive IO Means. The planner should ask, "What friendly Activities are most important to protect if the D-IO Objective is to be achieved?" The planner can base his evaluation on these factors: CC defensive guidance and values provided specifically for use in constructing the plan; or a review of previous plans and situations that contain information that can be adapted to the plan under construction. Of course, the individual planners' or planning teams' expertise provide an excellent basis for evaluation as well. Refer to the Activities/Functions section for a list of sample friendly Activities.

FORM 9. Generate the Defensive IO Tasks. **For each Activity, identify the Functions that most contribute to the conduct of the Friendly Activity.** An Activity can be broken down into its component parts, known as "**Functions**" in the JIODPP. The successful accomplishing of the friendly activity will depend more on some of these Functions than on others. On this form, list those Functions that most contribute to the activity's successful accomplishment. *It is these Functions that Defensive IO strives to protect.* Refer to the Activities/Functions section for a list of sample friendly Functions. Refer to the chart below to see examples of Functions associated with a Friendly Activity.



FORM 10. Generate the Defensive IO Tasks. **Identify the Effect that an opponent may try to induce on the selected function.** The range of Effects an opponent may attempt to induce on friendly Functions is summarized in the following:



Destroy = Damage done to the function is permanent, and all aspects of the function have been affected **OR** A function's operation is permanently impaired, and the damage extends to all facets of the function's operation.

Deny = Damage done to the function is only temporary, but all aspects of the function were affected **OR** A function's operation is impaired over the short term, but the damage extends to all facets of the function's operation.

Degrade = Damage done to the function is permanent, but only portions of the function were affected; that is, the function still operates, but not fully **OR** A function's operation is permanently impaired, but the damage does not extend to all facets of the function's operation.

Disrupt = Damage done to the function is temporary, and only portions of the function were affected **OR** A function's operation is impaired over the short term and the damage does not extend to all facets of the function's operation.

Mislead = creation of a false perception which leads the opposition to act in a manner detrimental to mission accomplishment while benefiting accomplishment of friendly objectives.

Influence = selected projection or distortion of the truth to persuade the opposition to act in a manner detrimental to mission accomplishment while benefiting accomplishment of friendly objectives.

Exploit = attempts to gather information that will enable opposition ability to conduct operations to induce other Effects.

Other = There may be other Effects desired, and this field is designed to allow for "write in" Effects.

FORM 11. Generate the Defensive IO Tasks. **Review the Effects possible on the selected Function.** This form allows you to review and assess the Effect(s) an opponent may attempt to induce on friendly Functions. It allows planners to get some sense of the magnitude of the overall problem confronting the Defensive IO planning effort.

1. Review each friendly function and determine if the selected adversary-induced Effects are appropriate. These Effects will become part of the Defensive IO Task Statement.
2. Next, review your selections to assess how the opponent may attempt to sequence or synchronize Effects. You should be considering how an opponent may attempt to sequence IO Effects (e.g., mislead, then destroy) or mass Effects on the IO objective/target. Massing in this context infers a mutually supporting strategy to use different Effects in rapid sequence to confuse or delay friendly response.

FORM 12. Generate the Defensive IO Tasks. **Identify the Defensive IO Means Sets most suitable to protect against the Effects possible.** On this form, list the Function to be protected and the Effect to be defeated. Now select the general Defensive IO Means Set most suitable for protecting against the Effects possible.

There are several general categories of Defensive IO means. These include:

- Information Assurance
- Operations Security
- Physical Security
- Counter-deception
- Counter-propaganda (Psychological Operations)
- Counterintelligence
- Electronic Warfare
- Special Information Operations

These general groupings of Defensive IO Means Sets are capable of defending against certain Effects.

Counter-Deception Means will defend against the **Mislead** Effect.

Counter-Propaganda (Psychological) Operations Means will defend against the **Influence** Effect.

Counterintelligence Means will defend against the Exploit Effect.

Information Assurance, Operations Security, Physical Security, Electronic Warfare and **SIO** Means can defend against the Disrupt, Deny, Degrade, and Destroy Effects.

A combination of Defensive IO Means sets may be necessary to defeat the array of Effects an adversary may attempt to induce.

FORM 13. Generate the Defensive IO Tasks. **Write a Defensive IO Task Statement.** On this form write a Defensive IO Task Statement based on the Friendly Activity and Function to be protected, the Effect to be defeated, and the Defensive IO Means that is most suitable for defending against the Effect an opponent may attempt to induce. The chart shows examples of properly completed Defensive IO Task Statements.

FORM 14. Generate the Defensive IO Tasks. **Assign the Defensive IO Tasks to the Components.** On this form, write in the Defensive IO Tasks. Determine primary and supporting responsibilities (e.g., Army primary, Air Force supporting). Fill in the function blocks associated with the tasks by entering the Component selected and a "P" or an "S" to denote primary or supporting. Example: under the Counter-deception Heading for Task 1 would be "Navy - P" if the Navy were the most appropriate/capable

Component to accomplish the Defensive IO Task. If supporting responsibilities were to be assigned, this notation would also be made in the block, e.g., "Air Force - S."

Step Three: Identify Assets to be Protected and Conduct Risk Assessment

Form 15: Identify the IO Assets to be Protected and Conduct Risk Analysis. **Identify the IO Assets – characterized as Hardware, Software, Wetware or Data assets – that must be protected to defeat/prevent the Effect an Opponent is attempting to induce on the Friendly Function.** On this form, write in the hardware, software, wetware or data assets associated with the function to be protected. Asset selection is, more often than not, a collaborative process. The participants in the process may include the J6, J3, J2, Services, agencies such as the Defense Information Systems Agency, Joint Warfare Analysis Center and others.

Many factors must be assessed when selecting assets. Ideally, the assets identified for further analysis should be known to play an important role in the successful operation of the function to be protected. The following chart illustrates the generic types of assets that can be found in the hardware, software, wetware and data categories.

FORM 16: Identify Assets to be Protected and Conduct Risk Analysis. **Confirm or refine Effects possible on Assets to be protected.** Use this form to refine the Effects an opponent may attempt to induce on the Assets to be protected. The analysis should consider the complete array of Effects possible (perhaps as a consequence of the physics involved) as well as Effects most likely to be induced because a given opponent has the capability to do so. The form contains analysis aids that facilitate planners' review of Effects and allow the charting of "influence paths" when mapping the relationships among potential wetware Assets. Use the "IO Effects" chart as an aid to confirm or refine Effects an opponent may attempt to induce on selected Assets. Use the "Derive Actor" chart to map command or reporting relationships between echelons or hierarchies, or within high-level staffs. After the review, complete the form by writing in the assets selected and the corresponding Effect to be defeated.

FORM 17: Identify Assets to be Protected and Conduct Risk Analysis. **Evaluate and select the hardware, software, wetware and data Assets associated with the function to identify the ones most critical to the function's success. Evaluate further to identify the ones most vulnerable to attack.**

Determining how **critical** a given asset is to a function's success should include an examination of three factors: **availability**, **reliability** and **timeliness**.

- How would the **availability** of this function be impaired if this Asset were affected?
- How would the **reliability** of this function be impaired if this Asset were affected?
- How would the **timeliness** of this function be impaired if this Asset were affected?

AVAILABILITY = Degree to which the Asset, if affected, would impair the availability of the Function.

RATING SYSTEM for Availability

LOW = The function's availability would be minimally impaired if this asset were affected.

MEDIUM = The Function's availability would be impaired if this asset were affected.

HIGH = The Function's availability would be seriously impaired if this asset were affected.

RELIABILITY = Degree to which the Asset, if affected, would impair the reliability of the Function.

RATING SYSTEM for Reliability

LOW = The Function's reliability would be minimally impaired if this asset were affected.

MEDIUM = The Function's reliability would be impaired if this asset were affected.

HIGH = The Function's reliability would be seriously impaired if this asset were affected.

TIMELINESS = Degree to which the Asset, if affected, would impair the timeliness of the Function.

RATING SYSTEM for Timeliness

LOW = The Function's timeliness would be minimally impaired if this asset were affected.

MEDIUM = The Function's timeliness would be impaired if this asset were affected.

HIGH = The Function's timeliness would be seriously impaired if this asset were affected.

FORM 18: Identify Assets to be Protected and Conduct Risk Analysis. **Evaluate the assets according to the criteria for impact of loss (critical).** Use the form to conduct the evaluations for the selected assets and derive values.

FORM 19: Identify Assets to be Protected and Conduct Risk Analysis. **Plot the "impact of loss" value for the evaluated Asset on the chart.** Use the form to plot the values derived for the selected assets.

FORM 20: Identify Assets to be Protected and Conduct Risk Analysis. **Evaluate the Assets according to the criteria for probability of loss (vulnerable).** Vulnerability is the degree to which a target is "open" to attack. Use the form to conduct the evaluations for the selected assets and derive values.

Determining how vulnerable a given Asset is to an opponent's attack should include an examination of five factors:

- Is the Asset **accessible**?
- Is the Asset **susceptible** to attack?
- Is it **feasible** to attack the Asset?
- What is the Opponent's **capability** to attack the Asset?
- What is the Opponent's **intent** with respect to an attack on the Asset?

ACCESSIBILITY = Degree to which the Asset can be "reached" by an attacking system.

RATING SYSTEM for Accessibility

LOW = access to Asset would be difficult to obtain.

MEDIUM = access to Asset can be gained.

HIGH = access to Asset is easily gained

SUSCEPTIBILITY = Degree to which the Asset can be affected.

RATING SYSTEM for Susceptibility

LOW = Asset can be affected by an attack to a limited degree at best.

MEDIUM = Asset can be affected by an attack.

HIGH = Asset can be highly affected by an attack

FEASIBILITY = An attack on this Asset can be accomplished; a measure of the feasibility associated with the attacking of the Asset.

RATING SYSTEM for Feasibility

LOW = The feasibility of attacking the Asset is low.

MEDIUM = The feasibility of attacking the Asset is medium.

HIGH = The feasibility of attacking the Asset is high.

CAPABILITY = A measure of the Opponent's ability to employ weapons systems/techniques to achieve a desired Effect on the Asset.

RATING SYSTEM for Capability

LOW = The opponent's capability to attack the asset is low.

MEDIUM = The opponent's capability to attack the target is medium.

HIGH = The opponent's capability to attack the target is high.

INTENT = A measure of the opponent's level of purpose in regards to attack on Friendly Assets. When assessing an Opponent's intent to attack an Asset, two factors can be considered:

STATEMENTS OF PURPOSE: Does the Opponent's public or official statements of policy or doctrine indicate that it would as a matter of course conduct attacks on these Assets; and

RELATED ACTIVITIES: Do related Opponent activities (troop movements, political activities, civil defense preparations, etc.) indicate that the Opponent intends to attack the Asset?

RATING SYSTEM for Intent

LOW = The opponent's intent to attack the asset is low.

MEDIUM = The opponent's intent to attack the asset is medium.

HIGH = The opponent's intent to attack the asset is high

FORM 21: Identify Assets to be Protected and Conduct Risk Analysis. **Plot the probability of loss value for the evaluated asset on the chart.** Use the form to plot the values derived for the selected assets.

FORM 22: Identify Assets to be protected and conduct Risk Analysis. **Plot the values derived for the selected asset during the Impact of loss/Probability of loss evaluations on their respective axes to display an overall value for risk.** Plot the values derived on Forms 18 and 20 for the selected asset onto Form 22. The impact of loss value from Form 18 is plotted on the "y" axis; the probability of loss value from Form 20 is plotted on the "x" axis. Where the two values would intersect on the chart, draw a star. The star represents graphically the combined numerical quantification of Risk posed to the asset.

Step Four: Select Protection Measures and Derive Defensive Information Operations Sub-tasks as Required

FORM 23: Select Protection Measures and Derive the Defensive IO Sub-tasks. **Identify the Specific Defensive IO Means most appropriate for diminishing the Risk posed by adversary-induced**

Effects on the selected critical and vulnerable assets; evaluate to select those most capable of diminishing the adversary-induced Effect on the asset. On this form, write the asset to be protected and the Effect to be defeated. Select specific D-IO assets that can diminish the adversary-induced Effect on the asset.

FORM 24: Select Protection Measures and Derive the Defensive IO Sub-tasks. **Evaluate the Defensive IO Means according to the criteria for diminishing impact of loss of a critical asset.** On this form, evaluate the ability of the D-IO Means to diminish the impact of the asset's loss on the availability, reliability, and timeliness of the associated Function. Write the D-IO asset to be employed at the top of the form. Evaluate the D-IO Mean's ability to diminish the impact of the Asset's loss on the availability, reliability and timeliness of the associated Function by using the criteria on the form. Use the form to conduct the evaluations and derive the values.

Determining the ability of a defensive IO Means to diminish the impact of the Asset's loss will again include an examination of three factors: **availability**, **reliability**, and **timeliness**.

- How would the D-IO Means diminish the impact of the Asset's loss on the **availability** of this function?
- How would the D-IO Means diminish the impact of the Asset's loss on the **reliability** of this function?
- How would the D-IO Means diminish the impact of the Asset's loss on the **timeliness** of this function?

AVAILABILITY = Degree to which the D-IO Means, when applied to the Asset, would improve the availability of the Function.

RATING SYSTEM for Availability

LOW = The Function's availability would be minimally improved if this D-IO Means were employed on this Asset.

MEDIUM = The Function's availability would be improved if this D-IO Means were employed on this Asset.

HIGH = The Function's availability would be significantly improved if this D-IO Means were employed on this Asset.

RELIABILITY = Degree to which the D-IO Means, when applied to the Asset, would improve the reliability of the Function.

RATING SYSTEM for Reliability

LOW = The Function's reliability would be minimally improved if this D-IO Means were employed on this Asset.

MEDIUM = The Function's reliability would be improved if this D-IO Means were employed on this Asset.

HIGH = The Function's reliability would be significantly improved if this D-IO Means were employed on this Asset.

TIMELINESS = Degree to which the D-IO Means, when applied to the Asset, would improve the timeliness of the Function.

RATING SYSTEM for Timeliness

LOW = The Function's timeliness would be minimally improved if this D-IO Means were employed on this Asset.

MEDIUM = The Function's timeliness would be improved if the is D-IO Means were employed on this Asset.

HIGH = The Function's timeliness would be significantly improved if this D-IO Means were employed on this Asset.

FORM 25: Select Protection Measures and Derive the Defensive IO Sub-tasks. **Plot the reduction in the impact of asset loss conferred by the D-IO Means.** On this form, plot the reduction in impact of loss. To do so, subtract the value derived for the reduction in impact of asset loss (Form 24) from the impact of asset loss value derived on Form 18 for the same asset. Plot this value on the chart.

FORM 26: Select Protection Measures and Derive the Defensive IO Sub-tasks. **Evaluate the D-IO Means according to the criteria for diminishing probability of loss of a vulnerable Asset.** On this form, calculate the reduction in probability of loss. Write the D-IO means being evaluated on the form. Evaluate the D-IO Mean's ability to diminish the **feasibility, susceptibility, and accessibility** of attack by the opponent; evaluate as well the D-IO Mean's ability to diminish the Opponent's **capability and intent** to attack the Asset. Use the form to conduct the evaluations and derive the values.

Determining how a specific D-IO Means will diminish an asset's probability of loss should include an examination of five factors:

- How will the D-IO Means diminish the Opponent's **accessibility** to the Asset?
- How will the D-IO Means diminish the **susceptibility** of the Asset to Opponent attack?
- How will the D-IO Means diminish the **feasibility** of the Opponent's attacking the Asset?
- How will the D-IO Means diminish the Opponent's **capability** to attack the Asset?
- How will the D-IO Means diminish the Opponent's **intent** to attack the Asset?

ACCESSIBILITY = Degree to which the opponent's ability to "reach" the asset can be diminished.

RATING SYSTEM for Accessibility

LOW = D-IO Means would not significantly diminish opponent accessibility to the Asset.

MEDIUM = D-IO means would diminish Opponent accessibility to Asset.

HIGH = D-IO Means would significantly diminish Opponent's accessibility to asset.

SUSCEPTIBILITY = Degree to which the Asset's ability to be affected by an Opponent's attack can be diminished.

RATING SYSTEM for Susceptibility

LOW = D-IO Means will not significantly diminish the Asset's susceptibility to attack.

MEDIUM = D-IO Means will diminish the Asset's susceptibility to attack.

HIGH = D-IO Means will significantly diminish the Asset's susceptibility to attack.

FEASIBILITY = Degree to which the feasibility of an attack on this asset can be diminished. When assessing a D-IO Means' ability to diminish the feasibility of an Opponent's attacking an Asset, three factors can be considered:

TECHNICAL: Does the D-IO Means diminish the Opponent's technical capabilities for attacking the Asset;

RESOURCES: Does the D-IO Means diminish the Opponent's ability to attack the asset with the minimum forces needed to be effective; and

TIME: Does the D-IO Means cause the Opponent to increase the time needed to attack the asset successfully?

RATING SYSTEM for Feasibility

LOW = The D-IO Means will not significantly diminish the feasibility of the Opponent's attacking the Asset.

MEDIUM = The D-IO Means will diminish the feasibility of the Opponent's attacking the Asset.

HIGH = The D-IO Means will significantly diminish the feasibility of the Opponent's attacking the Asset.

CAPABILITY = Degree to which an Opponent's capability to attack an Asset will be diminished. It is a measure of the Opponent's ability to employ weapons systems/techniques to achieve a desired Effect on the Asset. When assessing a D-IO Mean's ability to diminish an Opponent's capability to attack an Asset, two factors can be considered:

EFFICIENCY: Does the D-IO Means diminish the Opponent's ability to attack the Asset efficiently; and

SUCCESS: Does the D-IO Means diminish the Opponent's ability to attack the target successfully?

RATING SYSTEM for Capability

LOW = The D-IO Means will not significantly diminish the opponent's capability to attack the asset.

MEDIUM = The D-IO Means will diminish the opponent's capability to attack the asset.

HIGH = The D-IO Means will significantly diminish the opponent's capability to attack the asset.

INTENT = Degree to which an Opponent's level of purpose in regards to attack on Friendly Assets can be diminished. When assessing a D-IO Mean's ability to diminish an Opponent's intent to attack an Asset, two factors can be considered:

STATEMENTS OF PURPOSE: Does the D-IO Means alter the Opponent's public or official statements of policy or doctrine such that the potential for an attack on the Asset is diminished; and

RELATED ACTIVITIES: Does the D-IO Means seem to cause changes in related activities (troop movements, political activities, civil defense preparations, etc.) such that the Opponents intent to attack and Asset appears to be diminished?

RATING SYSTEM for Intent

LOW = The D-IO Means will not significantly alter the opponent's intent to attack the asset.

MEDIUM = The D-IO Means can alter the opponent's intent to attack the asset.

HIGH = The D-IO Means has a significant potential to alter the opponent's intent to attack the asset.

FORM 27: Select Protection Measures and Derive the Defensive IO Sub-tasks. **Plot the reduction in the probability of asset loss conferred by the D-IO Means.** On this form, plot the reduction in probability of asset loss. To do so, subtract the value derived for the reduction in probability of asset loss (Form 26)

from the probability of asset loss value derived on Form 20 for the same asset. Plot this value on the chart.

FORM 28: Select Protection Measures and Derive the Defensive IO Sub-tasks. **Plot the overall reduction in risk to the Asset conferred by the D-IO Means.** Plot the values derived on Forms 25 and 27 for the selected asset onto Form 28. The value representing the reduction in impact of Asset loss from Form 25 is plotted on the "y" axis; the value representing the reduction in probability of Asset loss from Form 27 is plotted on the "x" axis. Where the two values would intersect on the chart, draw a star. The star represents graphically the combined numerical quantification indicating the overall Reduction in Risk posed to the asset based on the D-IO Means applied.

FORM 29: Select Protection Measures and Derive the Defensive IO Sub-tasks. **Select Defensive IO Means-Asset combinations to minimize the Risk of Opponent-induced Effect.** On this form, pair Assets to be protected with the D-IO Means that most reduce the risk of Opponent-induced Effect.

FORM 30: Select Protection Measures and Derive the Defensive IO Sub-tasks. **Evaluate the selected Means-Asset combinations in light of Cost criteria.** On this form, use the criteria to derive a value representing the costs to protect the Asset with the D-IO Means identified.

Determining the value for cost to protect a specific Asset with a specific D-IO Means should include an examination of three factors:

- What are the *monetary* costs?
- What are the *political* costs?
- What are the *human* costs?

MONETARY = Dollar cost of employing D-IO Means.

RATING SYSTEM for Monetary

LOW = D-IO Means for protecting the Asset is low in cost.

MEDIUM = D-IO means for protecting the Asset is moderate in cost.

HIGH = D-IO Means for protecting the Asset is high in cost.

POLITICAL = Political cost of employing the D-IO Means.

RATING SYSTEM for Political

LOW = Political cost of employing the D-IO Means is low.

MEDIUM = Political cost of employing the D-IO means is moderate.

HIGH = Political cost of employing D-IO Means is high.

HUMAN = Human cost (casualties) of employing D-IO Means.

RATING SYSTEM for Human

LOW = Human cost of employing D-IO Means for protecting the Asset is low.

MEDIUM = Human cost of employing D-IO means for protecting the Asset is moderate.

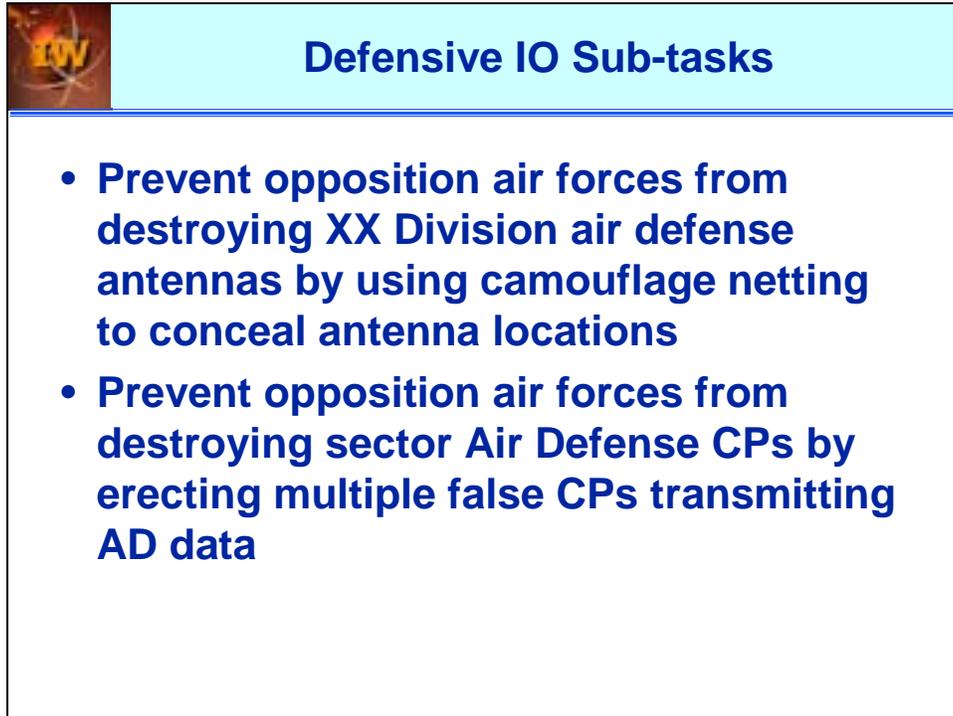
HIGH = Human cost of employing D-IO Means for protecting the Asset is high.

FORM 31: Select Protection Measures and Derive the Defensive IO Sub-tasks. **Select the final Means-Asset combinations by calculating Protection Value according to the formula as given on the form.** Use the form to make the calculation and determine the best Means-Asset combinations. The value for cost was derived in Form 30; Risk on Form 22; and Benefit on Form 28.

FORM 32: Select Protection Measures and Derive the Defensive IO Sub-tasks. **Derive and Write D-IO Sub-tasks.** The D-IO Sub-task statement is intended to be a clear statement of what is to occur. The IO Sub-task should include the following:

- The Effect to be defeated?
- The specific Asset to be protected?
- The specific D-IO Means to be applied?

The Chart below illustrates one such completed IO Sub-task:



Defensive IO Sub-tasks

- Prevent opposition air forces from destroying XX Division air defense antennas by using camouflage netting to conceal antenna locations
- Prevent opposition air forces from destroying sector Air Defense CPs by erecting multiple false CPs transmitting AD data

Step Five: Prepare the Master Protection List and Conduct Equity Review

FORM 33: Prepare the Master Protection List and Conduct Equity Review. **Prepare the candidate D-IO Master Protection List.** On this form, the candidate D-IO Master Protection List is assembled. On the form, list the Asset name; the coordinates/location; the IO Means to be applied; and the entity responsible for implementing the protective measures. Gather the information specified and write the information on the form.

FORM 34: Prepare the Master Protection List and Conduct Equity Review. **Review Defensive IO Sub-tasks in light of appropriate checklists to ensure that various equities are properly considered.** The review of equities is the final step in the Joint IO Defensive Planning Process. On this form, the various D-IO Sub-tasks are reviewed to ensure that they are checked against other factors that may bear on the defense of IO Assets. These other factors include the following.

Offensive versus Defensive – This dilemma is well known to most planners. An opponent may observe the “plugging” of friendly “holes” for defensive purposes. The opponent may then realize that the same or similar holes exist in his force structure. Opponent action to fix these holes will result in the loss of Friendly avenues of attack. The opposite situation is also true. Friendly exploiting of Opponent “holes” may cause an Opponent response on similar holes existing in Friendly force structure. Offense/Defense equities must be carefully balanced to insure that the net overall advantage accruing to friendly forces is as great as possible.

Joint Restricted Frequency Lists – The Joint Spectrum Center is principally responsible for the construction of these lists. The J6 will also be involved, as well as the J2. The IO planner is ensuring here that D-IO will not impact friendly attack communications or other operations negatively.

Security Compromise. This factor may become crucial if sensitive, perishable, high cost technologies are to be employed in the hope of achieving a specific defensive goal. The question here is “does the expected operational outcome justify the potential exposure of high cost, technically perishable technologies?” Alternatively, this factor could include an assessment of the risk of exposing D-IO methods and techniques that are or have been extremely effective, and whose utility may be completely neutralized if exposed.

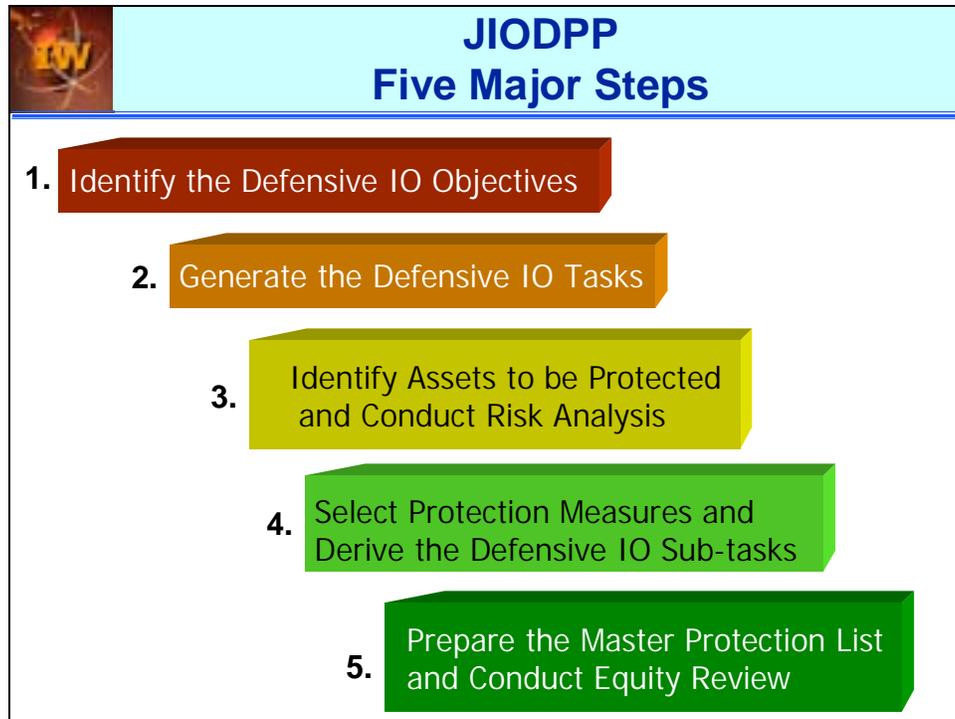
No Strike. This factor is designed to search for assets that, if defended, would cause an unacceptable level of unintended damage to another function or structure. The simplest example is one where an IO asset being defended is next to a hospital, school, or other non-combatant structure. An active defense or decoy may be employed that will cause the opponent to miss the Asset, but possibly cause collateral damage. Another example may be where a given D-IO Means is used to affect an adversary’s joint military-civil-commercial communications network that friendly forces may wish to preserve for other purposes.

Service. Service equities must be considered when finalizing D- IO plans. When D-IO Means are limited, a CC may choose to allocate defensive resources from one component to another where most needed.

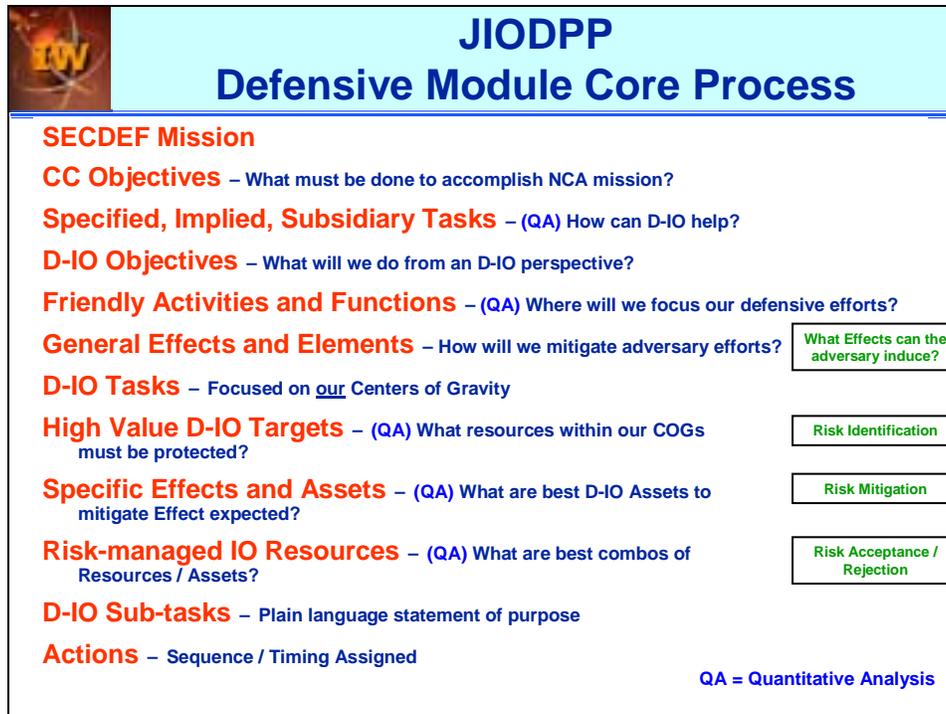
Once the equities are reviewed and adjusted, the candidate Master D-IO Protection List will be forwarded for de-confliction/integration with the Air Tasking Order and other attack orders. Once de-conflicted and integrated, it becomes the Master D-IO Protection List.

Class Slides

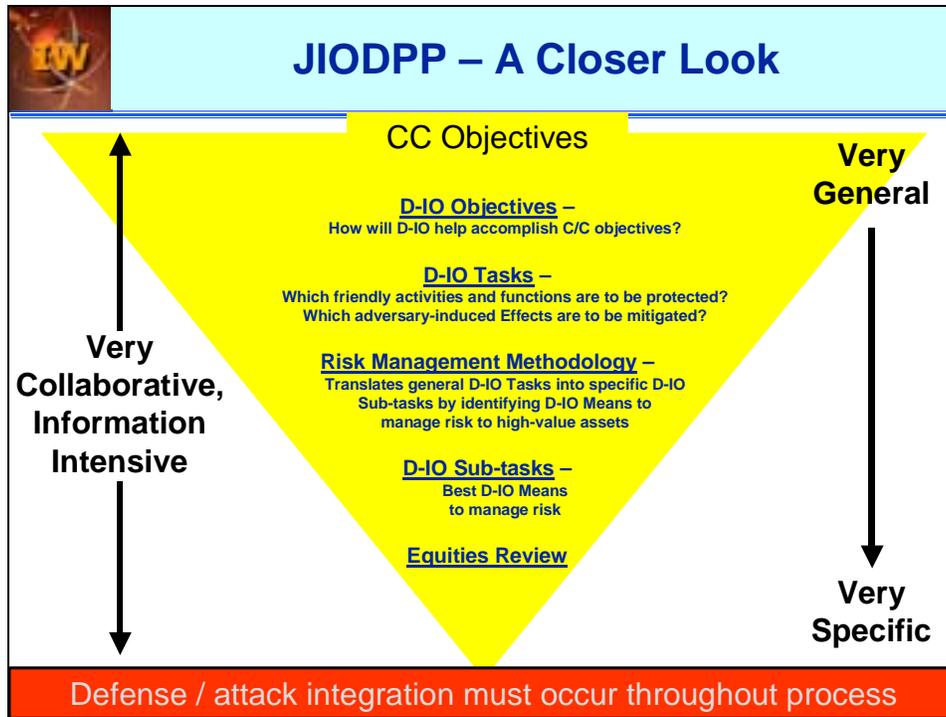
The following slides illustrate the key points of this chapter and are used as part of the Joint IO Planning Course class that covers IO planning.



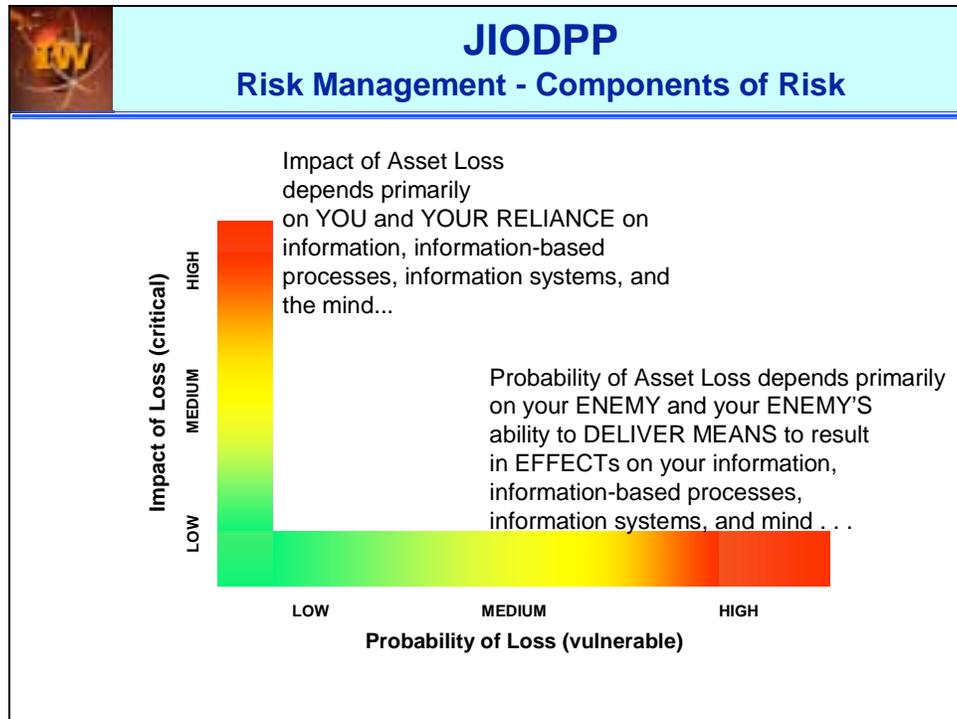
Now let's take a look at the JIODPP. The JIODPP is extremely flexible. While all five steps of the process should be accomplished, the level of detail, particularly in the third and fourth steps, may be varied based upon the amount of time available for planning.



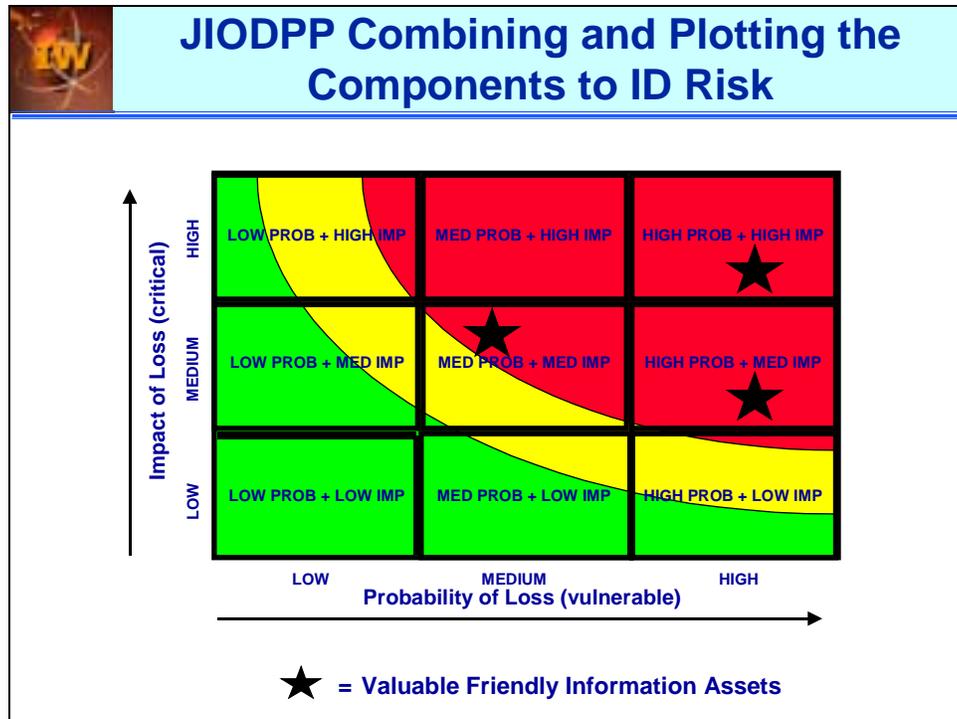
Putting the entire process on one chart, it looks something like this. We'll look at each of these steps.



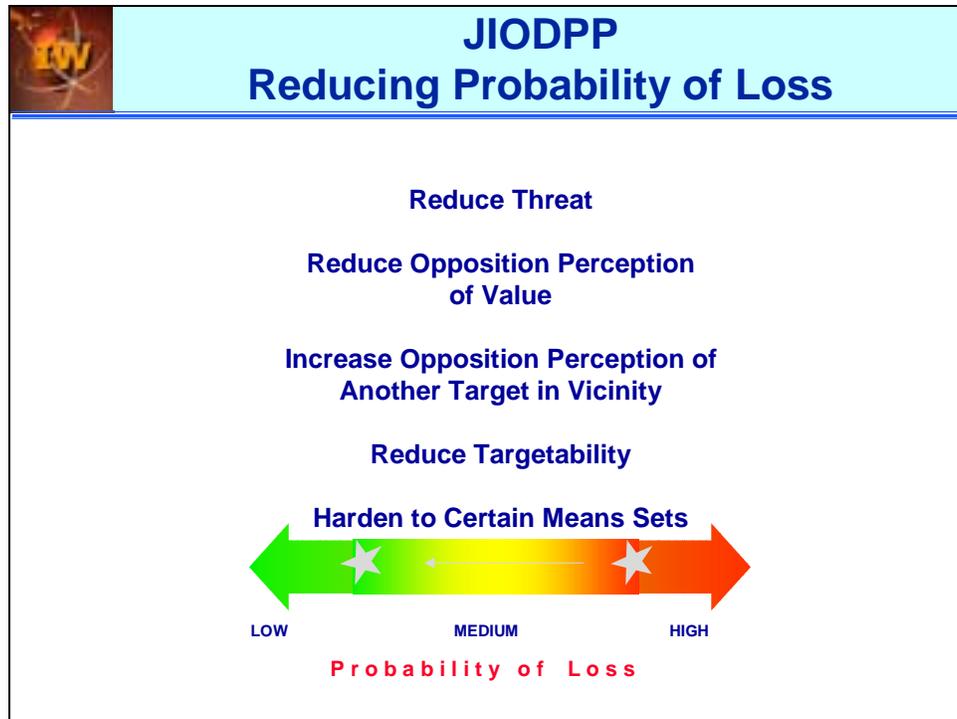
As you go through the JIODPP you will be required to identify high-value friendly information systems and then assess their vulnerability to attack by an adversary. This assessment will be used to conduct risk management.



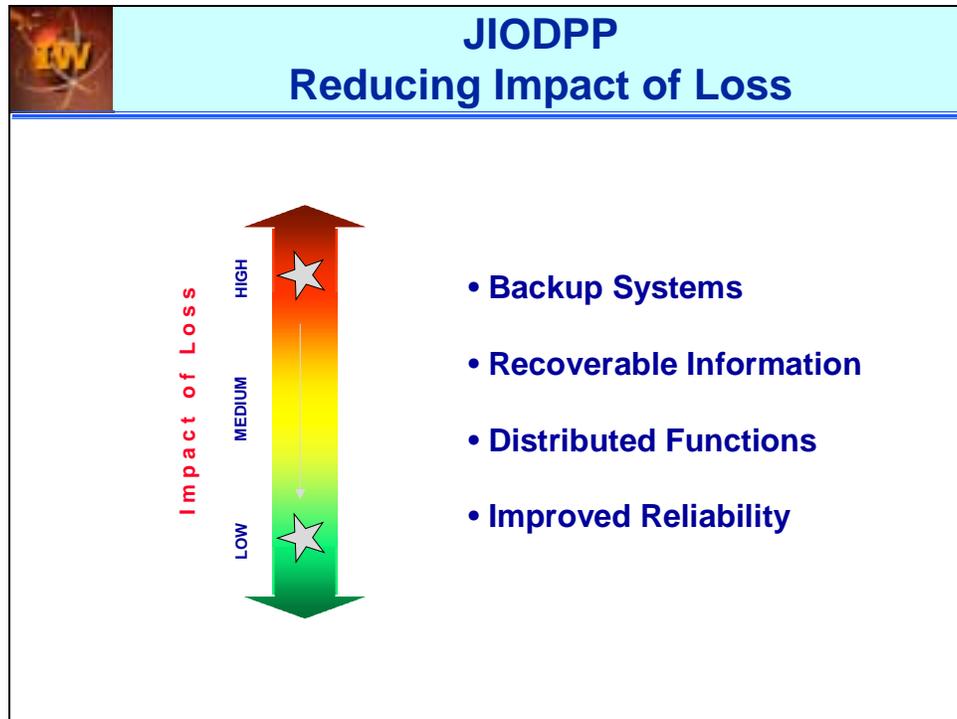
Once you identify the high value assets requiring protection, you must conduct risk management in order to prioritize your defensive IO activities and to develop means of defending your high-value assets. In conducting risk management you will consider two factors. The first factor is the impact of loss, which is shown on the Y-axis. The second factor is the probability of loss, shown on the X-axis.



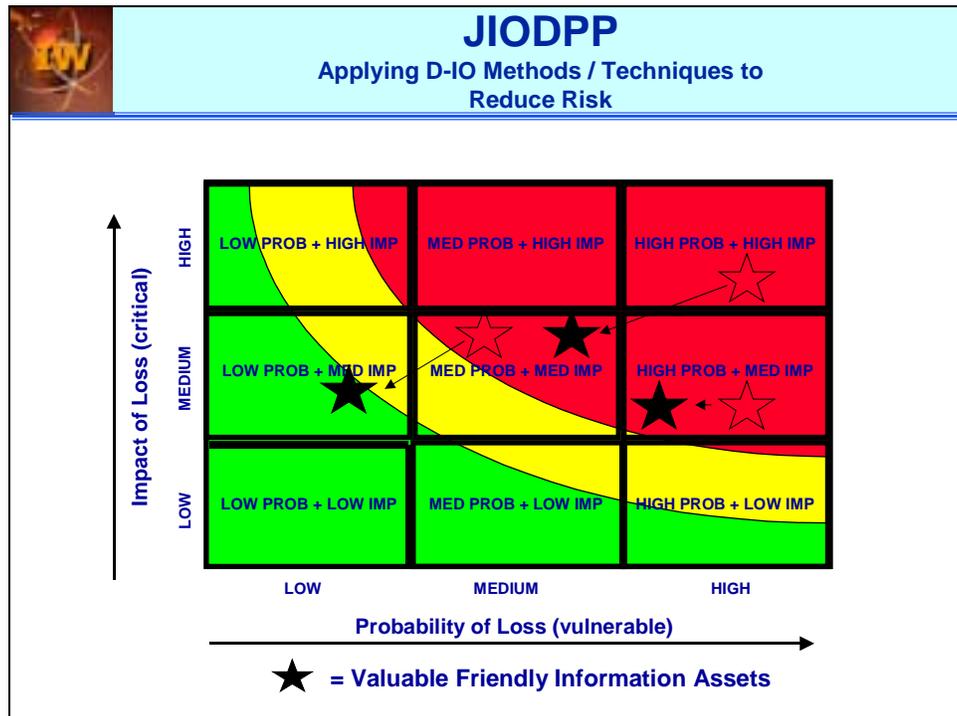
The JIODPP describes how to plot a risk assessment for each high value asset requiring protection that you identify. By plotting the risk for each high value asset, you will be better able to prioritize which assets require protection.



Once you prioritize the high value assets requiring protection, there are a number of measures that can be applied to reduce risk to teach system by reducing the probability of losing the asset. These measures include both physical protective measures and perception management measures.



Likewise, there are measures you may take to reduce the impact of the loss of a high value asset.



By reducing the probability of loss and the impact of loss for your high value assets, you can reduce the overall risk to the assets.

		JIODPP Equity Review				
		Defense / Offense / Intel	JRFL	Security Compromise	Open Asst	Service
Sub-task 1	✓	✓				
Sub-task 2	X	✓	X			
Sub-task 3						
Sub-task 4						
Sub-task 5						

Review D-IO Sub-tasks to ensure various equities are properly considered

The review of equities is the final step in the Joint IO Defensive Planning Process. On this form, the various D-IO Sub-tasks are reviewed to ensure that they are checked against other factors that may bear on the defense of IO Assets. These other factors include the following.

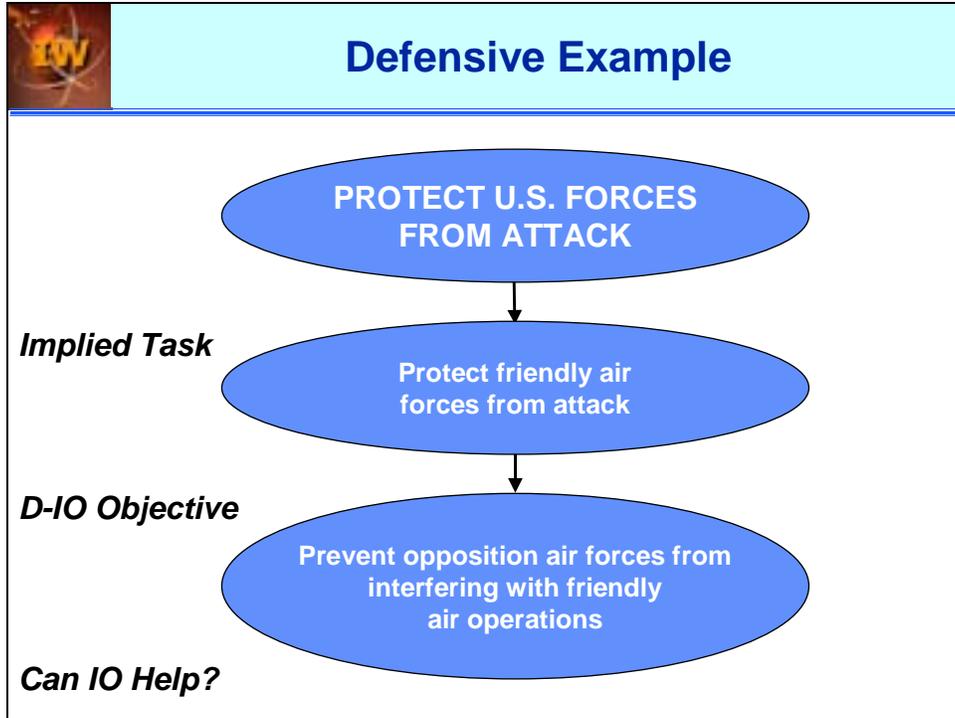
Offensive versus Defensive. This dilemma is well known to most planners. An opponent may observe the “plugging” of friendly “holes” for defensive purposes. The opponent may then realize that the same or similar holes exist in his force structure. Opponent action to fix these holes will result in the loss of Friendly avenues of attack. The opposite situation is also true. Friendly exploiting of Opponent “holes” may cause an Opponent response on similar holes existing in Friendly force structure. Offense/Defense equities must be carefully balanced to insure that the net overall advantage accruing to friendly forces is as great as possible.

Joint Restricted Frequency Lists. The Joint Spectrum Center is principally responsible for the construction of these lists. The J6 will also be involved, as well as the J2. The IO planner is ensuring here that D-IO will not impact friendly attack communications or other operations negatively.

Security Compromise. This factor may become crucial if sensitive, perishable, high cost technologies are to be employed in the hope of achieving a specific defensive goal. The question here is “does the expected operational outcome justify the potential exposure of high cost, technically perishable technologies?” Alternatively, this factor could include an assessment of the risk of exposing D-IO methods and techniques that are or have been extremely effective, and whose utility may be completely neutralized if exposed.

No Strike. This factor is designed to search for assets that, if defended, would cause an unacceptable level of unintended damage to another function or structure. The simplest example is one where an IO asset being defended is next to a hospital, school, or other non-combatant structure. An active defense or decoy may be employed that will cause the opponent to miss the Asset, but possibly cause collateral damage. Another example may be where a given D-IO Means is used to affect an adversary’s joint military-civil-commercial communications network that friendly forces may wish to preserve for other purposes.

Service. Service equities must be considered when finalizing D-IO plans. When D-IO Means are limited, a CC may choose to allocate defensive resources from one component to another where most needed. Once the equities are reviewed and adjusted, the candidate Master D-IO Protection List will be forwarded for de-confliction/integration with the Air Tasking Order and other attack orders. Once de-conflicted and integrated, it becomes the Master D-IO Protection List.





IO Navigator (ION)

- **Written in Java**
- **ION technically platform-independent, but optimized for PC-based Windows NT**
- **Uses ORACLE database**
- **Designed as a distributed, collaborative planning tool for networked use, but can be used in a stand-alone mode**
- **JWICS or SIPRNET communications backbones**
- **Runs best on a 266 MHz or faster processor; 128 MB or more of RAM is preferred**
- **ION release 2.0 operational 30 April 2001**

This page intentionally left blank

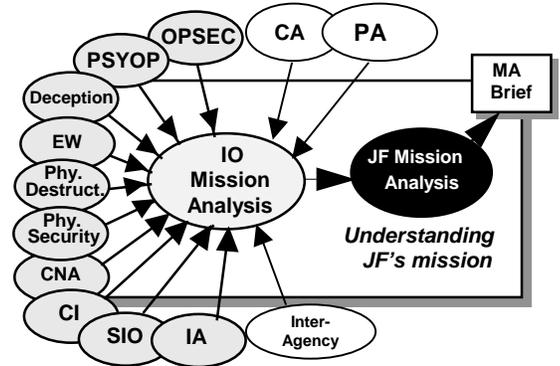
Chapter VII – Annexes and Appendices

Annex A – Information Operations Estimate Process

The first step in either crisis action or deliberate planning is the conduct of a mission analysis. All staff sections, including the IO cell, will examine the mission from their own perspective and contribute the results of that analysis to the core planning group. The following guide amplifies the steps outlined earlier in the planning handbook.

1. The IO mission analysis

- a. Determine known facts, current status, or conditions of joint IO/IW capabilities. Determine the size, capabilities, and status of IO-related forces apportioned for planning.
- b. Identify adversary information and information systems that enable the enemy to affect the JF. (J2, JIPB)
- c. Profile adversary leadership and their decision-making processes. (J-2, JIPB)
- d. Profile friendly leadership and their decision making processes and assess vulnerabilities. For example: Will your commander need to consult with coalition or national leadership prior to executing certain types of activities? To what degree will media attention and public reaction have on key decision-makers?
- e. Develop assumptions to replace missing facts.
 - (1) Make only assumptions needed to continue planning.
 - (2) Do not assume away an adversary's capability.
 - (3) Track your assumptions and attempt to validate as soon as possible.
- f. Determine IO constraints (must do) and restraints (cannot do).
 - (1) Themes and messages provided from the interagency may fit this category.
 - (2) Broadcast activities may be limited due to political sensitivities in neighboring countries or due to terrain and weather characteristics.
- g. Analyze friendly and enemy COGs and determine Critical Vulnerabilities that IO can affect both offensively and defensively.
 - (1) List the COG to be analyzed.
 - (2) List the COG's critical capabilities (CC). CCs are defined as those adversary or friendly capabilities that are considered crucial enablers for the COG to function as such, and are essential to the accomplishment of your or the adversary's assumed objective(s).
 - (3) List the Critical Requirements (CR) for each CC. CRs are those essential conditions, resources, and means for a critical capability to be fully operational.
 - (4) Identify, if present, Critical Vulnerabilities (CV). CVs are those aspects or components of the critical capabilities (or components thereof), which are deficient, or vulnerable to neutralization, interdiction, or attack in a manner achieving decisive or significant results, disproportionate to the military resources applied. One must have the operational reach to affect these CVs otherwise they cannot be targeted.
- h. Identify IO related tasks (specified, implied, and essential).
 - (1) Specified Tasks are those tasks specifically stated in the planning directive.
 - (2) Implied Tasks are tasks not specifically assigned, but that must be performed to accomplish the mission.
 - (3) Essential Tasks are those tasks, gleaned from the specified and implied tasks, that must be performed to achieve overall mission success.
- i. Determine which IO capabilities (don't forget the Inter-Agency) may be utilized to accomplish the IO tasks. The purpose of this step is to gain a rough assessment of the IO resources that will be needed to accomplish the mission and to begin to visualize how the capabilities and related activities will be utilized.



- j. Assess initial IO risks and develop mitigation strategies as appropriate.
 - k. Develop recommended Commander's Critical Information Requirements (CCIR). The CCIR is a comprehensive list of information requirements identified by the commander as being critical in facilitating timely information management and the decision-making process that affect successful mission accomplishment. (JP 5-00.2) It has two key subcomponents.
 - (1) Priority Intelligence Requirements (PIR): Those intelligence requirements for which a commander has an anticipated and stated priority in the task of planning and decision-making. (JP 2-0)
 - (2) Essential Elements of Friendly Information (EEFI): Key questions likely to be asked by adversary officials and intelligence systems about specific friendly intentions, capabilities, and activities, so they can obtain answers critical to their operational effectiveness. (JP 1-02)
 - l. Provide results of IO mission analysis to the core planning group.
2. **Receive Commander's planning guidance:** The commander should provide guidance at this point. Planning guidance should be disseminated to the IO/IW Cell's personnel and the components. If needed, ask the commander for any guidance necessary for continued planning.
3. **Course of Action Development:** The JF staff should now develop multiple friendly COAs. The below steps should be conducted by the IO cell concurrent with the core planning staff's COA development efforts. The IO cell representative to the core planning staff who keeps the IO cell apprised of the larger COA development effort and ensures that the efforts and findings of the IO cell are incorporated into the larger COA development effort.
- a. Review mission analysis and commander's planning guidance.
 - b. Develop IO objectives, sub-objectives and supporting MOEs that support accomplishment of the commander's objectives. Time-phase the IO Objectives.
 - (1) **Objective**
 - (a) The clearly defined, decisive, and attainable goals towards which every military operation should be directed.
 - (b) The specific target of the action taken.
 - (c) For example, a definite terrain feature, the seizure or holding of which is essential to the commander's plan, or, an enemy force or capability without regard to terrain features.
 - (d) Source: JP 1-02
 - (2) **Objective Characteristics**
 - (a) An objective must be observable, achievable (or attainable) and quantifiable (or measurable).
 - 1 Observable. The objective must strive for some visible change.
 - 2 Achievable. The assets and time available are sufficient to accomplish the objective.
 - 3 Quantifiable. The change must be related to some quantifiable end goal.
 - (b) The following questions should be answered when defining an objective:
 - 1 What can IO do to help achieve the commander's objectives? The specific goal (rather than a generalized or notional goal) must be identified. For example, do you wish to modify the behavior of a political leader, military force, the civilian population, or any combination of the three?
 - 2 Against whom? Identify the activity that is to be affected, changed or modified.
 - 3 The purpose. Why do you want to achieve the objective? There is always a "why." Not understanding the "why" may result in analysis and recommendations that neither meet the commander's needs nor are effective as they could or should be.
 - 4 How much (to what degree) do you want to affect the activity? State any criteria against which progress and success will be measured. Criteria must use quantifiable terms and be realistic. They can include when and for how long we want to impact the objective and where we want to affect the adversary activity.

- 5 How much will it cost to achieve the objective and is it worth the cost?
- (3) **How to Write an IO Objective**
- (a) Writing an IO Objective is a 3-step process and it follows the EFFECT + TARGET + PURPOSE format.
- (b) Step 1: Choose the Target
- 1 The JIOC target categories are as follows:
- (i) Hardware (e.g. physical targets such as C3 facilities, information systems, etc.)
 - (ii) Software (e.g. programs that run on computers)
 - (iii) Wetware (e.g. military and political decision makers, population groups)
- 2 Information Targets can also be grouped as follows:
- (i) Physical space (e.g. traditional fixed and mobile targets)
 - (ii) Electronic space (e.g. the airwaves, data that moves on the Internet and GCCS)
 - (iii) Perception space (e.g. the decision making processes of military and political decision makers and population groups)
- (c) Step 2: Determine the effect you want to achieve
- 1 The effect is a clearly defined action that you want individuals or organizations to achieve. A reference list is provided in Annex B: IO Effects Definitions. If you decide to use another "effect" word, you must define it to avoid confusion.
- (d) Step 3: Determine the purpose
- 1 The purpose is the "why" we want to achieve this objective. Just like kinetic targeting, every objective has a "why." By clearly stating the why, the IO planner ensures strategy to task linkage. The purpose portion starts off with the phrase "in order to" and then adds one of the following words with an elaboration
- (i) Allow
 - (ii) Cause
 - (iii) Create
 - (iv) Enable
 - (v) Support
- 2 NOTE: The purpose in the IO objective statement can be omitted if the purpose of the objective is glaringly obvious. If the objective is "Deter NLAM aggression", you might not need to state the purpose of the objective.
- 3 Example: Influence NLAM leadership to refrain from attacking relief operations personnel in order to ensure the safety of relief operations personnel. (In this example, the "in order" is somewhat obvious and would likely be omitted.)
- (4) **Measures of Effectiveness (MOE)**
- (a) Definitions
- 1 Tools used to measure results achieved in the overall mission and assigned tasks. Measures of effectiveness are a prerequisite to the performance of combat assessment. (JP 1-02)
- 2 Subjective indicators that the outcomes of tactical actions have achieved or contributed to achieving the desired effect. Measures of effectiveness articulate where to look and what to measure in order to determine if the desired effect has been achieved. (JFCOM Glossary)
- (b) Combat Assessment
- 1 Determination of the overall effectiveness of force employment during military operations. Combat assessment is composed of three major components:
- (i) Battle damage assessment
 - (ii) Munitions effectiveness assessment
 - (iii) Re-attack recommendation
- 2 Source: JP 3-60
- (c) MOE Characteristics
- 1 Focused on assessing the achievement of the objective
- 2 Measurable and observable: Quantitative values or qualitative descriptions
- 3 Timely and responsive: Collection and analysis is rapid enough to support timely decision-making.
- 4 Cost effective

- (d) How to develop an IO MOE
 - 1 Step 1: Develop the MOE statement. Use the objective's target, effect, and purpose as a guide to determine what must be observed, reported, and assessed.
 - 2 Step 2: Develop the leading indicators that support the MOE statement. Leading indicators are quantifiable signs that measure trends or progress towards attaining the objective. The IO planner should wargame potential leading indicators that will assist in measuring achievement of the IO objective. This is normally done in conjunction with the J2 representative to the IO cell and other members of the IOWG. The purpose of developing indicators is to:
 - (i) Establish a baseline of activity from which success or lack of progress can be measured. All indicators should have a baseline of activity from which to measure progress.
 - (ii) Assist the J2 in determining intelligence collection requirements.
 - (iii) Focus the other members of the staff and the components to potential collection requirements.
 - 3 The IO cell's job is to make known the intelligence requirements and establish a mechanism for tracking progress on accomplishing the objectives.
 - 4 Example
 - (i) Statement: NLAM leadership is influenced to not attack relief operations personnel.
 - (ii) Indicators:
 - 1. Decrease in the number of kidnappings or attempted kidnappings of disaster relief personnel
 - 2. Decrease in the number of attacks on U.S. Military personnel
 - 3. Reduction in the number of NLAM threatening phone calls to the US embassy
 - 4. NLAM leadership changes rhetoric in open press
 - 5. NLAM leadership increases contact with third party envoy
 - 6. Intercepts of NLAM leadership communications directing no aggression
- c. Coordinate with the J-2 on collection requirements related to your MOEs and indicators.
- d. Examine the adversary and friendly force structures and determine where to focus IO efforts to achieve the IO objectives. The COG analysis performed during mission analysis is a good starting point for this step. That analysis should have led you to develop those critical capabilities and critical requirements that are most vulnerable to IO capabilities.
- e. Determine what effect you want to have on the most critical and vulnerable functions and select the IO capability or capabilities that can best achieve that effect.
 - (1) Analyze the initial force structure to determine if the apportioned forces roughly possess adequate IO capabilities.
 - (2) Identify any shortfalls.
- f. Write IO tasks and assign them to an appropriate component. Time-phase the tasks.
 - (1) The format for writing a task statement is EFFECT + TARGET + PURPOSE + CAPABILITY.
 - (2) Step 1: Identify the Target – The IO planner needs to ID the critical node(s), decision-maker(s) or group(s) that the IO capability or related activity is going to execute this task against.
 - (3) Step 2: Identify the Effect – Identify the effect you want to achieve against this target. This will not necessarily match up with the effect found in the IO objective. For example, to influence someone, you might expose something, destroy something and inform that person of something else.
 - (4) Step 3: Select the IO Capability or Related Activity – Select the IO capability or related activity that best achieves the effect you want to achieve with regards to the target. The phrasing portion of the statement starts off with "by employing (fill in the IO capability or related activity).
 - (5) Step 4: Fill in the "why" you are doing this task – This is normally a direct lift of the "why" found in the IO Objective or Sub-Objective that the task is supporting.
 - (6) Step 5: Write the task statement – Use the format: EFFECT + TARGET + PURPOSE + CAPABILITY
 - (7) Step 6: Assign the task to the appropriate component.

- (8) Examples:
 - (a) Influence NLAM Leadership not to attack relief operations personnel using PSYOP.
 - (b) Deny NLAM Leadership EEFI in order protect relief operations personnel using IA / OPSEC / CNO / EW.
 - (c) Inform village leaders that support NLAM of humanitarian nature of the relief operation in order protect relief operations personnel using CA / PA / PSYOP / Inter-Agency.
 - g. Select the target(s) that are most critical and vulnerable. (Done in concert with the tasked component.)
 - h. Confirm and deconflict effects desired on target selected. This deconfliction must first take place within the IO cell, but like all other IO related actions, must be deconflicted with all other elements of the joint force.
 - i. Select the best asset-target pairs to attack. (Typically performed by the tasked component.)
 - j. Write and time-phase the IO sub-task. (Typically performed by the tasked component.)
 - k. Compile the IO target list.
 - l. In concert with the ROE cell or JAG representative, assess ROE implications of IO activities and adjust as required.
 - m. Participate in COA development with the core planning staff. Ensure that all IO related actions are synchronized with those of the other components. Also deconflict IO targets with those of the other components. Ensure that any adversary assets that you intend to exploit or use for IO related purposes are on the no strike or restricted target list. This is typically done within a Targeting working group or a Joint Targeting Coordination Board or equivalent forum.
4. **Participate in COA analysis (war gaming).** Be prepared to contribute to the process of war-gaming by mentally “fighting the battle” in time and space. The process may use the structure of action-reaction-counteraction sequences for critical events (e.g. D-Day actions). Key elements the staff is determining include more details about:
- a. Specific tasks for components with IO/IW capabilities
 - b. Command relationships
 - c. Decision points for IO/IW
 - d. Operational support needed
 - e. Identification of branches (what if) and sequels (what then)
5. **Participate in COA comparison**
- a. Participate in determining the criteria to be used for comparing COAs. Criteria for IO/IW operations could come from:
 - (1) Commander’s Intent.
 - (2) Factors of METT-T (+)
 - (a) Mission accomplishment
 - (b) Adversary
 - (c) Terrain
 - (d) Troops available
 - (e) Time available
 - (f) Political
 - b. Ensure recommendations for IO/IW operations have been coordinated with the components of the JF.
6. **Receive CJF’s decision on COAs.** The CJF may select or modify the recommended COA. Based on that decision, the Commander’s Estimate document (or slides) will normally be sent/briefed to the CC for approval.
7. **Provide input/develop IO/IW perspective in JF plan/order.** After the COA is selected, the plan/order is physically developed. Most of the information needed for this task should have already been developed through the estimate process (mission analysis through COA selection).
- a. After you have selected a COA, you can write the IO concept of operations.

- (1) The IO concept of operations is a written statement that gives an overall picture of how IO will support the operation. JOPEs says that the IO planner should summarize how the commander visualizes the execution of IO from the beginning to termination.
 - (2) Describe how IO will support the command's operational mission.
 - (3) Summarize the concepts for supervision and termination of IO.
 - (4) Summarize the JFC's purpose for the operation or phase
 - (a) This is found in the first part of the JFC's Intent paragraph.
 - (b) State in general terms how IO will support the overall concept of operations / phase. This statement should focus of the "what" (effects), not the "who" (IO capabilities and related activities). This portion of the paragraph starts with "IO will support this by _____."
 - (c) Summarize the JFC's endstate for the operation or termination criteria for the phase.
 - (5) The concept of operations may be a single paragraph or divided into two or more paragraphs depending on the complexity of the operation. The concepts for offensive and defensive IO may be addressed in separate paragraphs.
- b. IO/IW operations input can be in many sections of the plan/order, however, the primary areas for writing IO/IW information are in the following portions per JOPEs (see CJCSM 3122.03):
- (1) Information Operations – Appendix 3 (Information Operations) to Annex C (Operations).
 - (2) Deception Operations – Tab A (Military Deception) of Appendix 3 to Annex C.
 - (3) Electronic Warfare – Tab B (Electronic Warfare) of Appendix 3 to Annex C.
 - (4) Operations Security – Tab C (Operations Security) of Appendix 3 to Annex C.
 - (5) Psychological Operations – Tab D (Psychological Operations) of Appendix 3 to Annex C.
 - (6) Physical Destruction – Tab E (Physical Attack/Destruction) of Appendix 3 to Annex C.
 - (7) Computer Network Attack – Tab F (CNA) of Appendix 3 to Annex C, and/or Annex S (STO).
 - (8) Defensive IO/IW – Tab G (Defensive Information Operations) of Appendix 3 to Annex C.
 - (9) Other areas in which IO/IW is included in the plan/order include:
 - (a) Intelligence – Annex B (Intelligence)
 - (b) Public Affairs – Annex F (Public Affairs)
 - (c) Civil Affairs – Annex G (Civil Affairs)
 - (d) Communications – Annex K (Command, Control, Communications and Computer Systems)
 - (e) Space Operations – Annex N (Space)
 - (f) Consequence Management – Annex T (Consequence Management)
 - (g) Interagency – Annex V (Interagency Coordination)
 - (h) Execution– Annex X (Execution Checklist)

Appendix 1 – Operations Security

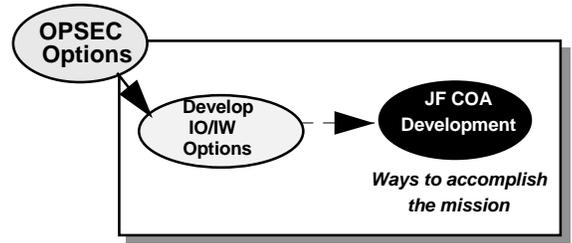
1. Contribute to JF's overall mission analysis

- a. Determine known facts, current status, or conditions of joint OPSEC as defined in the CC's planning document (Planning Order, Operations Order, etc.).
- b. Identify "critical information."
 - (1) Determine Essential Elements of Friendly Information (EEFI).
 - (2) Determine "critical information" (a subset of EEFI). This is the information vitally needed by the adversary and focuses the remainder of the OPSEC planning process (see JP 3-54, Appendix A for examples).
- c. Analyze the adversary. Work with intelligence and counterintelligence staffs to answer the following:
 - (1) Who is the adversary? (Those with intent and capability to take action against the planned operation.)
 - (2) What are the adversary's goals?
 - (3) What is the adversary's strategy for opposing the planned operation?
 - (4) What critical information does the adversary already know about the operation?
 - (5) What are the adversary's intelligence collection capabilities (or Hostile Intelligence System (HOIS) collection capabilities)?
- d. Analyze vulnerabilities (see JP 3-54, Appendix C for "OPSEC Indicators").
 - (1) What indicators (friendly actions and open source information) of critical information not known to the adversary will be created by the friendly activities generated by the planned operation?
 - (2) What is the adversary's ability to collect against these indicators?
 - (3) What indicators will the adversary be able to use to the disadvantage of friendly forces?
 - (4) Friendly indicators of EEFI.
 - (a) Signatures.
 - (b) Associations.
 - (c) Profiles.
 - (d) Contrasts.
 - (e) Exposure.
- e. Conduct a risk assessment. Review risk assessment done by the entire JPG. The following questions should be asked continuously throughout the planning process.
 - (1) What risk to effectiveness is likely to occur if a particular OPSEC measure is implemented?
 - (2) What risk to mission success is likely to occur if an OPSEC measure is not implemented?
 - (3) What risk to mission success is likely if an OPSEC measure is not implemented or fails?
- f. Develop assumptions to replace missing or unknown facts concerning OPSEC.
- g. Determine OPSEC limitations.
 - (1) Things that OPSEC must do (constraints).
 - (2) Things OPSEC cannot do (restraints).
 - (3) Others (e.g., political, weather, terrain, etc.).
- h. Identify OPSEC tasks to be performed by JF forces.
 - (1) Determine specified tasks.
 - (2) Determine implied tasks.
 - (3) Determine subsidiary tasks.
 - (4) From (1), (2) and (3) above, determine essential tasks or goals.
- i. Assist in development of JF mission statement, if appropriate.
- j. Assist in development of mission analysis briefing for the CJF.
- k. Integrate all efforts through coordination with other members of the IO/IW Cell.

2. Receive CJF planning guidance. CJF should provide guidance at this point. Planning guidance should be disseminated to OPSEC personnel and the components. If needed, ask the CJF for any guidance necessary for continued planning.

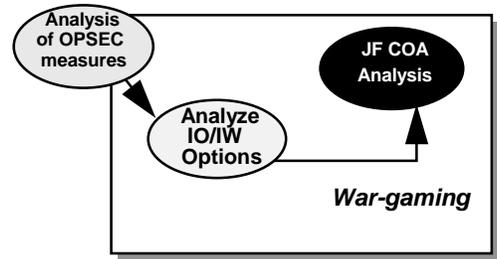
3. **Develop OPSEC options to support the JF's COAs.** The JF staff should now develop multiple friendly COAs.

- a. Develop OPSEC options for initial JF COAs.
 - (1) Review mission analysis and CJF's guidance.
 - (2) Develop specific OPSEC measures to support the JF's COAs from the beginning of the operation to the end in the following areas (see JP 3-54, Appendix D):
 - (a) Operational measures.
 - (b) Logistics measures.
 - (c) Technical measures.
 - (d) Administrative measures.
 - (e) Military deception in support of OPSEC.
 - (f) Physical destruction in support of OPSEC.
 - (g) Electronic warfare in support of OPSEC.
- b. Coordinate ROE with JF ROE cell for each OPSEC measure.
- c. Plan to incorporate OPSEC elements in the JF information architecture.
- d. Develop the general concept for implementation of OPSEC measures. Describe by operational phase and major activity (maneuver, logistics, communications, etc.).
- e. Determine coordination requirements for:
 - (1) OPSEC coordination measures between JF components.
 - (2) Public affairs coordination.
 - (3) Guidance on termination of OPSEC-related activities.
 - (4) Guidance on declassification and public release of OPSEC-related activities.
 - (5) Administrative and logistics support of OPSEC-related activities.
 - (6) Command and control measures.
 - (a) Feedback mechanisms.
 - 1 Monitoring the effectiveness of OPSEC measures during execution.
 - 2 Specific intelligence requirements for feedback.
 - (b) OPSEC surveys.
 - (c) After-action reports.
 - (d) Signals. OPSEC-related communications requirements.
- f. Provide input to JF COA statement and sketches.



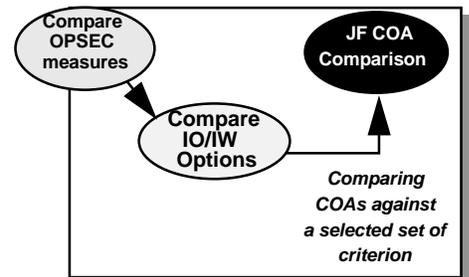
4. **Participate in COA analysis (war gaming).** Be prepared to contribute to the process of war-gaming by mentally "fighting the battle" in time and space. The process may use the structure of action-reaction-counteraction sequences for critical events (e.g., D-Day actions). Key elements the staff is determining include more details about:

- a. Specific tasks for components in the OPSEC area.
- b. Decision points for OPSEC measures.
- c. Operational support needed.
- d. Identification of branches (what if) and sequels (what then).



5. **Participate in COA comparison.**

- a. Participate in determining the criteria for comparing JF COAs. Criteria for OPSEC measures could come from:
 - (1) Commander's Intent.
 - (2) Factors of METT-T.
 - (a) Mission accomplishment.
 - (b) Adversary.
 - (c) Terrain.
 - (d) Troops available.
 - (e) Time available.



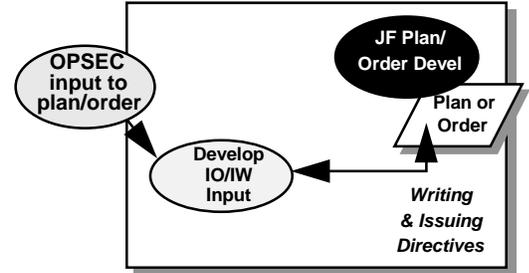
b. Ensure recommendations for OPSEC measures have been coordinated with the components of the JF.

6. **Receive CJF's decision on COAs.**

The CJF may select or modify the recommended COA. Based on that decision, the Commander's Estimate document (or slides) will normally be sent/briefed to the CC for approval.

7. **Provide input/develop OPSEC perspective in JF plan/order.** After the COA is selected, the plan/order is physically developed. Most of the information needed for this task should have already been developed through the estimate process (mission analysis through COA selection). OPSEC input can be in many sections of the plan/order, however, the primary areas for writing OPSEC information are found in the following areas of JOPES (see CJCSM 3122.03):

- a. Paragraph 3 (Execution) of Appendix 3 (Information Operations) to Annex C (Operations).
- b. Tab C (Operations Security) of Appendix 3 to Annex C (Operations).



This page intentionally left blank

Appendix 2 – Psychological Operations

1. **Contribute to JF's overall mission analysis**

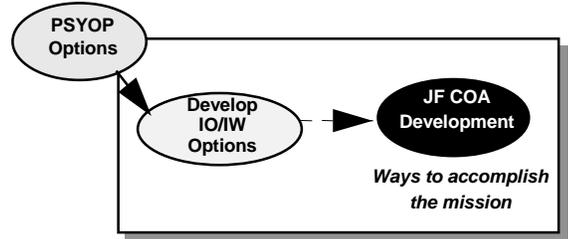
- a. Determine known facts, current status, or conditions of joint PSYOP forces as defined in the CC's planning document (Planning Order, Operations Order, etc.).
- b. In coordination with the J2, conduct analysis of the adversary's:
 - (1) Decision makers and staff.
 - (a) Decision makers who can direct development or allocation of adversary resources.
 - (b) Decision makers' characteristics.
 - (c) Decision makers' perceptions/preconceived notions about friendly operations.
 - (2) Intelligence Systems. Intelligence systems that support the adversary.
 - (3) Target audiences.
 - (a) Groups that can influence plans, decisions, and operational effectiveness of the adversary?
 - (b) Goals of these groups.
 - (c) Susceptibility of these groups to PSYOP.
 - (4) Adversary command systems.
 - (a) C4 structures of the adversary.
 - (b) Adversary structures vulnerable to PSYOP jamming or attacking.
- c. Analyze CC's mission and PSYOP objectives.
- d. Develop assumptions to replace missing or unknown facts concerning JF PSYOP operations.
- e. Determine PSYOP limitations.
 - (1) Things that PSYOP must do (constraints).
 - (2) Things PSYOP cannot do (restraints).
 - (3) Others (e.g., political, weather, terrain, etc.).
- f. Determine adversary and own center(s) of gravity (COGs) and tentative decisive points.
 - (1) Determine PSYOP-based approaches to adversary COGs.
 - (2) Determine ways for PSYOP to assist in protecting friendly force COGs.
- g. Identify PSYOP tasks to be performed by JF forces.
 - (1) Determine specified tasks.
 - (2) Determine implied tasks.
 - (3) From (1) and (2) above, determine essential tasks or goals.
- h. Conduct initial JF IW force structure analysis to determine if sufficient IW assets are available to do the tasks.
- i. Conduct a risk assessment. Review risk assessment done by the entire JPG. The following questions should be asked continuously throughout the planning process.
 - (1) What risk to effectiveness is likely to occur if a particular PSYOP measure is implemented?
 - (2) What risk to mission success is likely to occur if a PSYOP measure is not implemented?
 - (3) What risk to mission success is likely if a PSYOP measure fails to be effective?
- j. Determine end state from an IW perspective.
- k. Assist in development of JF mission statement.
- l. Assist in development of mission analysis briefing for the CJF.
- m. Integrate all efforts through coordination with other members of the IO/IW Cell.

2. **Receive CJF planning guidance.** CJF should provide guidance at this point. Planning guidance should be disseminated to PSYOP personnel and the components. If needed, ask the CJF for any guidance necessary for continued planning. Guidance should be sought on:

- a. Valid PSYOP themes to be promoted.
- b. Valid or invalid PSYOP themes to be avoided or discouraged.

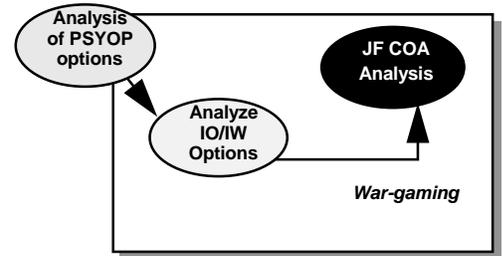
3. **Develop PSYOP options to support the JF's COAs.** The JF staff should now develop multiple friendly COAs.

- a. Develop PSYOP options for initial JF COAs.
 - (1) Review mission analysis and CJF's guidance.
 - (2) Develop specific PSYOP options that include:
 - (a) Target audience.
 - (b) PSYOP objectives, overall themes, and specific themes.
 - (c) Provisions for testing, producing, stocking, and disseminating PSYOP materials.
 - (d) Means to measure PSYOP effectiveness.
 - (e) Command and control arrangements.
 - (f) Logistics support requirements.
 - (g) OPSEC provisions to maintain secrecy of the commander's PSYOP intent.
 - (3) Develop specific tasking to the JF's components.
- b. Coordinate ROE with JF ROE cell for each PSYOP measure.
- c. Plan to incorporate PSYOP elements in the JF information architecture.
- d. Develop the general concept for implementation of PSYOP measures. Describe by operational phase and major activity (maneuver, logistics, communications, etc.).
- e. Determine coordination requirements for:
 - (1) PSYOP coordination measures between JF components.
 - (2) Public affairs coordination.
 - (3) Guidance on termination of PSYOP-related activities.
 - (4) Guidance on declassification and public release of PSYOP-related activities.
 - (5) Administrative and logistical support of PSYOP-related activities.
 - (6) Command and control measures.
 - (a) Feedback mechanisms.
 - 1 Monitoring the effectiveness of PSYOP measures during execution.
 - 2 Specific intelligence requirements for feedback.
 - (b) Signals. PSYOP-related communications requirements and code words.
- f. Provide input to JF COA statement and sketches.



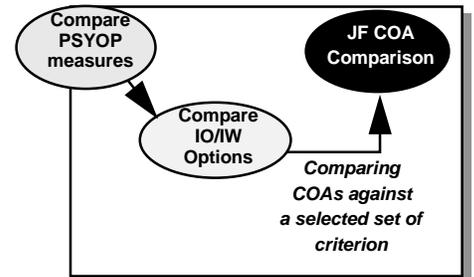
4. **Participate in COA analysis (war gaming).** Be prepared to contribute to the process of war-gaming by mentally "fighting the battle" in time and space. The process may use the structure of action-reaction-counteraction sequences for critical events (e.g. D-Day actions). Key elements the staff is determining include more details about:

- a. Specific tasks for components in the PSYOP area.
- b. Decision points for PSYOP measures.
- c. Operational support needed.
- d. Identification of branches (what if) and sequels (what then).



5. **Participate in COA comparison.**

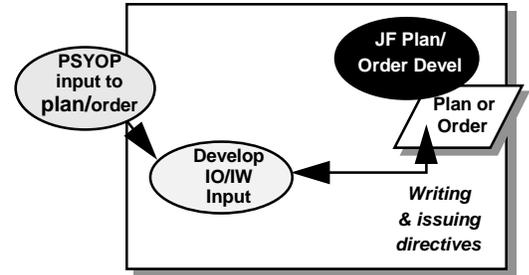
- a. Participate in determining the criteria for comparing JF COAs. Criteria for PSYOP measures could come from:
 - (1) Commander's Intent.
 - (2) Factors of METT-T.
 - (a) Mission accomplishment.
 - (b) Adversary.
 - (c) Terrain.
 - (d) Troops available.
 - (e) Time available.
- b. Ensure recommendations for PSYOP measures have been coordinated with the components of the JF.



6. **Receive CJF's decision on COAs.** The CJF may select or modify the recommended COA. Based on that decision, the Commander's Estimate document (or slides) will normally be sent/briefed to the CC for approval.

7. **Provide input/develop PSYOP perspective in JF plan/order.** After the COA is selected, the plan/order is physically developed. Most of the information needed for this task should have already been developed through the estimate process (mission analysis through COA selection). PSYOP input can be in many sections of the plan/order, however, the primary areas for writing PSYOP information are found in the following portions of JOPES (see CJCSM 3122.03):

- a. Para 3 (Execution) of Appendix 3 (Information Operations) to Annex C (Operations).
- b. Tab D (Psychological Operations) of Appendix 3 to Annex C.



This page intentionally left blank

Appendix 3 – Deception

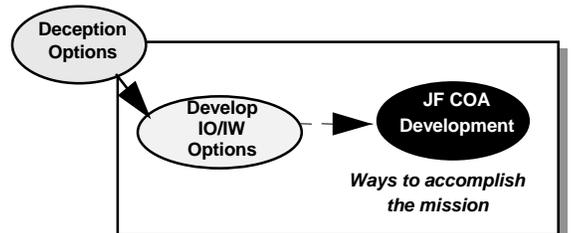
1. Contribute to JF's overall mission analysis

- a. Determine known facts, current status, or conditions of joint forces capable of deception operations as defined in the CC's planning document (Planning Order, Operations Order, etc.).
- b. In coordination with the J2, conduct analysis of the adversary.
 - (1) General adversary capabilities relating directly to the planning of deception.
 - (2) Deception targets.
 - (3) Deception target biases and predispositions.
 - (4) Probable adversary courses of action.
- c. Develop assumptions to replace missing or unknown facts concerning deception operations.
 - (1) Status of forces at probable execution.
 - (2) Available time.
 - (3) Other as appropriate.
- d. Analyze CC's mission and intent from a deception perspective.
- e. Determine deception operations limitations.
 - (1) Things the deception operations must do (constraints).
 - (2) Things the deception operations cannot do (restraints).
 - (3) Others (e.g., political, weather, terrain, etc.).
- f. Determine adversary and own center(s) of gravity (COGs) and tentative decisive points.
 - (1) Determine deception-based approaches to adversary COGs.
 - (2) Determine ways for deception to assist in protecting friendly force COGs.
- g. Identify tasks to be performed by deception capable JF forces.
 - (1) Determine specified deception tasks.
 - (2) Determine implied deception tasks.
 - (3) From (1) and (2) above, determine essential deception tasks or goals.
 - (a) Establish broad deception (offensive) goals.
 - (b) Establish broad counter-deception (defensive) goals.
- h. Conduct initial JF force structure analysis to determine if sufficient assets are available to do the tasks.
- i. Conduct an initial deception risk assessment. Review risk assessment done by the entire JPG. The following questions should be asked continuously throughout the planning process.
 - (1) Deception is successful. What will be the adversary's likely response? Subsequent impact on friendly forces?
 - (2) Deception fails. What will the impact be if the deception target ignores the deception or fails to take the intended actions?
 - (3) Deception is compromised. What will be the impact?
- j. Determine end state from a deception perspective.
- k. Assist in development of JF mission statement.
- l. Assist in development of mission analysis briefing for the CJF.

2. Receive CJF planning guidance. CJF should provide guidance at this point (see Task 202). Planning guidance should be disseminated to the deception personnel and the components. If needed, ask the CJF for any guidance necessary for continued planning.

3. Develop deception options to support the JF's COAs. The JF staff should now develop multiple friendly COAs.

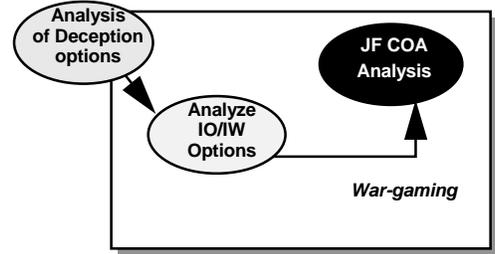
- a. Develop deception options for initial JF COAs.
 - (1) Review mission analysis and CJF's guidance.
 - (2) Develop deception options to support the JF's COAs from the beginning of the operation to the end by accomplishing the following:
 - (a) Determine desired perception.
 - 1 Reinforce existing belief/establish new



5. **Participate in COA comparison**

a. Participate in determining the criteria for comparing COAs. Criteria for deception operations could come from:

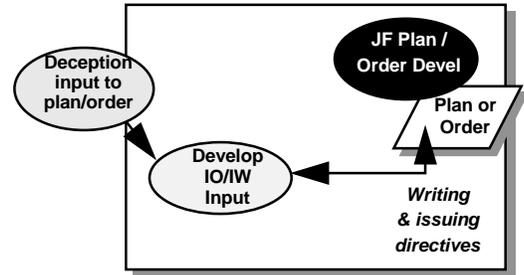
- (1) Commander's Intent
- (2) Factors of METT-T
 - (a) Mission accomplishment
 - (b) Adversary
 - (c) Terrain
 - (d) Troops available
 - (e) Time available



b. Ensure recommendations for deception operations have been coordinated with the components of the JF.

6. **Receive CJF's decision on COAs.** The CJF may select or modify the recommended COA. Based on that decision, the Commander's Estimate document (or slides) will normally be sent/briefed to the CC for approval.

7. **Provide input/develop deception perspective in JF plan/order.** After the COA is selected, the plan/order is physically developed. Most of the information needed for this task should have already been developed through the estimate process (mission analysis through COA selection). Deception operations input can be in many sections of the plan/order, however, the primary areas for writing deception operations information are found in the following portions of JOPES (see CJCSM 3122.03):



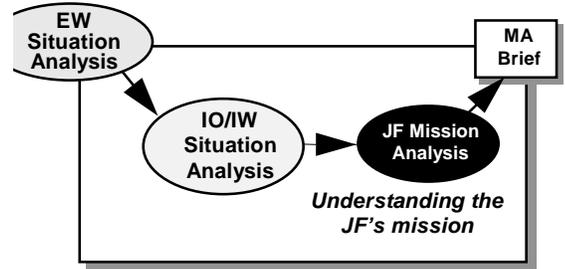
- a. Paragraph 3 (Execution) of Appendix 3 (Information Operations) to Annex C (Operations).
- b. Tab A (Deception) of Appendix 3 to Annex C.

This page intentionally left blank

Appendix 4 – Electronic Warfare

1. Contribute to JF's overall mission analysis

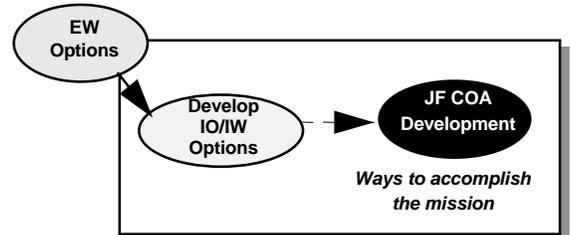
- a. Determine known facts, current status, or conditions of joint forces capable of EW operations as defined in the CC's planning document (Planning Order, Operations Order, etc.).
- b. In coordination with the J2, conduct analysis of the adversary.
 - (1) Determine adversary dependence on use of the electromagnetic spectrum.
 - (2) Determine adversary EW capability.
 - (3) Determine Hostile Intelligence System (HOIS) collection capability (see deception and OPSEC mission analysis).
 - (4) Determine adversary vulnerabilities related to use of the electromagnetic spectrum.
 - (5) Determine friendly vulnerabilities related to use of the electromagnetic spectrum.
- c. Develop assumptions to replace missing or unknown facts concerning EW operations.
 - (1) Status of forces at probable execution.
 - (2) Available time.
 - (3) Other as appropriate.
- d. Analyze CC's mission and intent from an EW perspective.
- e. Determine EW operations limitations.
 - (1) Things the EW operations must do (constraints).
 - (2) Things the EW operations cannot do (restraints).
 - (3) Others (e.g., political, weather, terrain, etc.).
- f. Determine adversary and own center(s) of gravity (COGs) and tentative decisive points.
 - (1) Determine EW-based approaches to adversary COGs.
 - (2) Determine ways for EW to assist in protecting friendly force COGs.
- g. Identify tasks to be performed by EW forces (Electronic Warfare Support (ES), Electronic Attack (EA), Electronic Protection (EP)).
 - (1) Determine specified EW tasks.
 - (2) Determine implied EW tasks.
 - (3) From (1) and (2) above, determine essential EW tasks or goals.
- h. Conduct initial JF EW force structure analysis to determine if sufficient assets are available to do the tasks.
- i. Conduct an initial EW risk assessment. Review risk assessment done by the entire JPG.
- j. Determine end state from an EW perspective.
- k. Assist in development of JF mission statement.
- l. Assist in development of mission analysis briefing for the CJF.



2. Receive CJF planning guidance. CJF should provide guidance at this point. Planning guidance should be disseminated to EW personnel and the components. If needed, ask the CJF for any guidance necessary for continued planning.

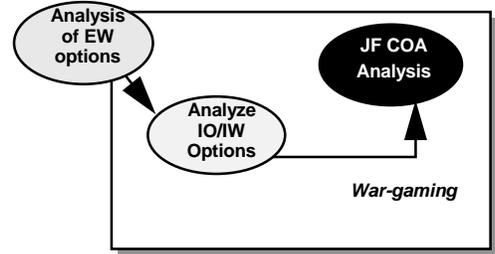
3. Develop EW options to support the JF's COAs. The JF staff should now develop multiple friendly COAs.

- a. Develop EW options for initial JF COAs.
 - (1) Review mission analysis and CJF's guidance.
 - (2) Develop EW options to support the JF's COAs for Electronic Warfare Support (ES).
 - (a) Plan ES for IW-O.
 1. Develop combat information for immediate targeting of adversary emitters.



- 2 Develop combat information for rapid feedback of effectiveness of joint force counter-IW operations.
 - 3 Develop combat information for further analysis as SIGINT.
 - (b) Plan ES for protection of friendly information, C2 and C4I (IW-D).
 - 1 Develop combat information for immediate targeting of adversary IW-O means.
 - 2 Use ES to support Indications and Warning (I&W) of adversary attack and adversary avoidance.
 - (3) Plan Electronic Attack (EA) in support of IW.
 - (a) Protect (IW-D) friendly use of the Electromagnetic Spectrum (EMS), by planning aggressive tactical jamming operations to cumulatively degrade adversary RSTA capability and other use of the EMS.
 - (b) Plan electromagnetic deception in support of military deception operations to confuse adversary RSTA efforts for both IW-O and IW-D.
 - (c) Plan EA, using Anti-Radiation Munitions (ARM) to degrade, neutralize or destroy adversary personnel or equipment for both IW-O and IW-D.
 - 1 Establish/recommend high priority targets for component use of destructive EA means.
 - 2 Integrate ARMs with jamming, stealth, Precision Guided Munitions (PGM), and Direct Action (DA) missions to counter adversary radar defenses.
 - (4) Plan Electronic Protection (EP) in support of IW (coordinate with the Information Assurance plan).
 - (a) Plan EP for IW to include Signals Security (SIGSEC) to prevent adversary exploitation of friendly use of the EMS.
 - (b) Use equipment that maximizes efficiency of friendly use of the EMS.
 - (c) Develop and implement procedures that promote operational efficiency in use of the EMS.
 - (d) Coordinate with the J6/frequency manager for development of the Joint Restricted Frequency List (JRFL).

4. **Participate in COA analysis (war gaming).** Be prepared to contribute to the process of war-gaming by mentally “fighting the battle” in time and space. The process may use the structure of action-reaction-counteraction sequences for critical events (e.g., D-Day actions). Analyze EW concept; war game within the context of other IW operations COAs and the overall JF operational COA (actual COAs developed by operational planners may provide basis for EW COAs). Determine:

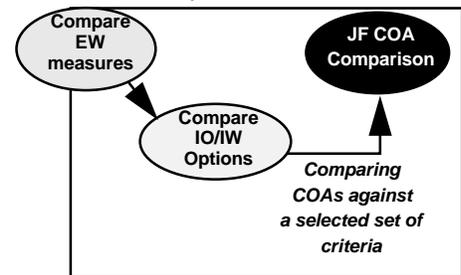


- a. More specific forces required.
- b. More specific assets/resources required.
- c. Possible branches (what if) and sequels (what then) to military EW requirements.
- d. Assess military EW risks.
- e. Unintended effects.
- f. Provide input to Time-Phased Force and Deployment Data (TPFDD) development to facilitate execution of EW plan in accordance with the overall JF plan.

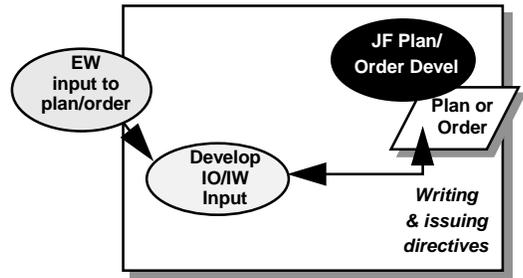
5. **Participate in COA comparison**

a. Participate in determining the criteria for comparing COAs. Criteria for EW operations could come from:

- (1) Commander’s Intent
- (2) Factors of METT-T
 - (a) Mission accomplishment
 - (b) Adversary
 - (c) Terrain
 - (d) Troops available
 - (e) Time available



- b. Ensure recommendations for EW operations have been coordinated with the components of the JF.
- 6. **Receive CJF's decision on COAs.** The CJF may select or modify the recommended COA. Based on that decision, the Commander's Estimate document (or slides) will normally be sent/briefed to the CC for approval.
- 7. **Provide input/develop EW perspective in JF plan/order.** After the COA is selected, the plan/order is physically developed. Most of the information needed for this task should have already been developed through the estimate process (mission analysis through COA selection). EW operations input can be in many sections of the plan/order, however, the primary areas for writing EW operations information are found in the following portions of JOPES (see CJCSM 3122.03):
 - a. Para 3 (Execution) of Appendix 3 (Information Operations) to Annex C (Operations).
 - b. Tab B (Electronic Warfare) of Appendix 3 to Annex C.

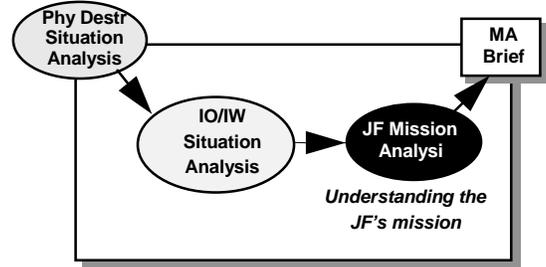


This page intentionally left blank

Appendix 5 – Physical Destruction

1. Contribute to JF's overall mission analysis

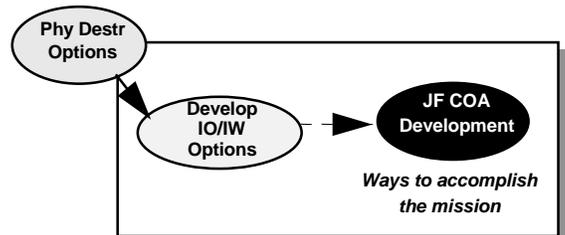
- a. Determine known facts, current status, or conditions of joint forces capable of physical destruction.
- b. In coordination with the J2, conduct analysis of the adversary.
- c. Develop assumptions to replace missing or unknown facts concerning physical destruction operations.
- d. Analyze CC's mission and intent from an physical destruction perspective.
- e. Determine physical destruction operations limitations.
 - (1) Things the physical destruction operations must do (constraints).
 - (2) Things the physical destruction operations cannot do (restraints).
 - (3) Others (e.g., political, weather, terrain, etc.).
- f. Determine adversary and own center(s) of gravity (COGs) and tentative decisive points.
 - (1) Determine approaches to adversary COGs.
 - (2) Determine ways to assist in protecting friendly force COGs.
- g. Identify tasks to be performed by physical destruction forces.
 - (1) Determine specified physical destruction tasks.
 - (2) Determine implied physical destruction tasks.
 - (3) From (1) and (2) above, determine essential physical destruction tasks or goals.
- h. Conduct *initial* JF physical destruction force structure analysis to determine if sufficient assets are available to do the *tasks*.
- i. Conduct an *initial* physical destruction risk assessment. Review risk assessment done by the entire JPG.
- j. Determine end state from an physical destruction perspective.
- k. Assist in development of JF mission statement.
- l. Assist in development of mission analysis briefing for the CJF.



2. Receive CJF planning guidance. CJF should provide guidance at this point. Planning guidance should be disseminated to IO/IW Cell personnel and the components. If needed, ask the CJF for any guidance necessary for continued planning.

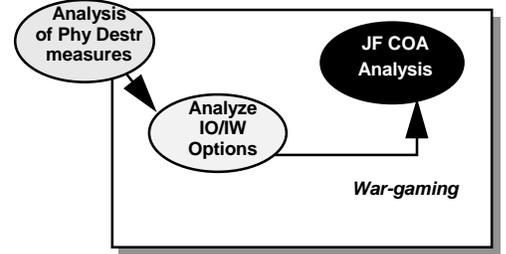
3. Develop physical destruction options to support the JF's courses of action. The JF staff should now develop multiple friendly COAs.

- a. Develop physical destruction options for initial JF COAs.
 - (1) Review mission analysis and CJF's guidance.
 - (2) Develop physical destruction options to support the JF's COAs.
 - (a) Plan destruction operations for IW-O (coordinate with J3, J2T and J3 fires element on overall JF targeting plan). Plan destruction against adversary information, C2 and C4I.
 - 1 Target adversary commanders, staff, communications and intelligence production facilities, consistent with military deception objectives.
 - 2 Destruction is timed for when adversary needs assets in decision cycle.
 - 3 Target control nodes to degrade effective support of decision cycles or dissemination of information.
 - 4 Target information (C2 and C4I) that indirectly affects specific control nodes.



- (b) Plan destruction operations for protection of friendly, information, C2, C4I(IW-D); integrate destruction with other IW elements to preclude disruption or contradiction of other operations (coordinate with J3, J2T and J3 fires element on overall JF targeting plans).

- 4. **Participate in COA analysis (war gaming).** Be prepared to contribute to the process of war-gaming by mentally “fighting the battle” in time and space. The process may use the structure of action-reaction- counteraction sequences for critical events (e.g., D-Day actions). Analyze physical destruction concepts; war game within context of other IW operations COAs and the overall JF operational COA (actual COAs developed by operational planners may provide basis for physical destruction COAs). Determine:

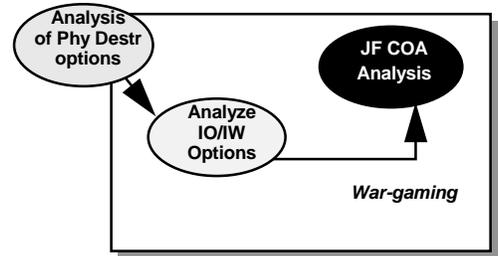


- a. More specific forces required.
- b. More specific assets/resources required.
- c. Possible branches (what if) and sequels (what then) to military physical destruction requirements.
- d. Assess military physical destruction risks.
- e. Unintended effects.
- f. Provide input to Time-Phased Force and Deployment Data (TPFDD) development to facilitate execution of physical destruction plan in accordance with the overall JF plan.

- 5. **Participate in COA comparison.**

- a. Participate in determining the criteria for comparing COAs. Criteria for physical destruction operations could come from:

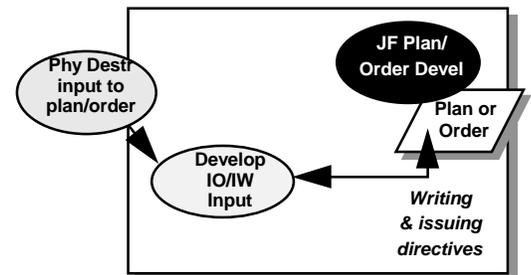
- (1) Commander’s Intent
- (2) Factors of METT-T
 - (a) Mission accomplishment
 - (b) Adversary
 - (c) Terrain
 - (d) Troops available
 - (e) Time available



- b. Ensure recommendations for physical destruction operations have been coordinated with the components of the JF.

- 6. **Receive CJF’s decision on COAs.** The CJF may select or modify the recommended COA. Based on that decision, the Commander’s Estimate document (or slides) will normally be sent/briefed to the CC for approval.

- 7. **Provide input/develop physical destruction perspective in JF plan/order.** After the COA is selected, the plan/order is physically developed. Most of the information needed for this task should have already been developed through the estimate process (mission analysis through COA selection). Physical destruction operations input can be in many sections of the plan/order, however, the primary areas for writing physical destruction operations information are found in the following portions of JOPES (see CJCSM 3122.03):

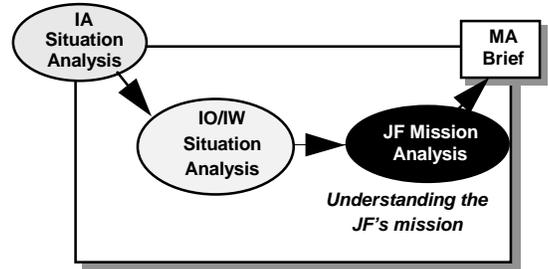


- a. Para 3 (Execution) of Appendix 3 (Information Operations) to Annex C (Operations).
- b. Tab E (Physical Attack/Destruction) of Appendix 3 to Annex C.

Appendix 6 – Information Assurance

1. Contribute to JF's overall mission analysis

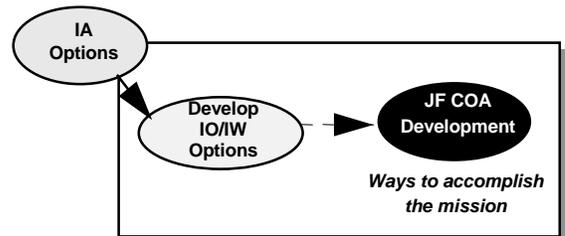
- a. Determine known facts, current status, or conditions of joint forces capable of IA.
- b. In coordination with the J2, conduct analysis of the adversary.
 - (1) Determine adversary dependence on use of the electromagnetic spectrum.
 - (2) Determine adversary communications attack and computer network attack capability.
 - (3) Determine Hostile Intelligence System (HOIS) collection capability (see deception and OPSEC mission analysis).
 - (4) Analyze friendly C2 and C4I for vulnerabilities related to use of the computer network attack and communications attack.
- c. Develop assumptions to replace missing or unknown facts concerning IA.
- d. Analyze CC's mission and intent from an IA perspective.
- e. Determine IA operations limitations.
 - (1) Things IA must do (constraints).
 - (2) Things IA cannot do (restraints).
 - (3) Others (e.g., political, weather, terrain, etc.).
- f. Determine adversary and own center(s) of gravity (COGs) and tentative decisive points.
 - (1) Determine approaches to adversary COGs.
 - (2) Determine ways to assist in protecting friendly force COGs.
- g. Identify tasks to be performed by IA forces.
 - (1) Determine specified IA tasks.
 - (2) Determine implied IA tasks.
 - (3) From (1) and (2) above, determine essential IA tasks or goals.
- h. Conduct initial JF IA force structure analysis to determine if sufficient assets are available to do the tasks.
- i. Conduct an initial IA risk assessment. Review risk assessment done by the entire JPG.
- j. Determine end state from an IA perspective.
- k. Assist in development of JF mission statement.
- l. Assist in development of mission analysis briefing for the CJF.



2. Receive CJF planning guidance. CJF should provide guidance at this point. Planning guidance should be disseminated to IO/IW Cell personnel and the components. If needed, ask the CJF for any guidance necessary for continued planning.

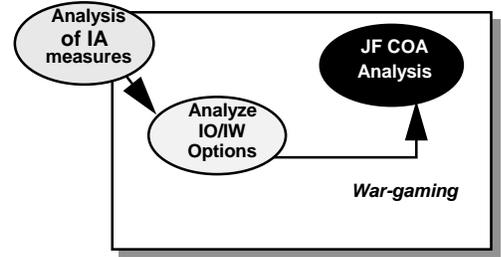
3. Develop IA options to support the JF's COAs. The JF staff should now develop multiple friendly COAs.

- a. Develop IA options for initial JF COAs.
 - (1) Review mission analysis and CJF's guidance.
 - (2) Develop IA options to support the JF's COAs. Plan IA operations for protection of friendly C2 and C4I. Integrate IA with other IW elements to preclude disruption of JF information, C2 and C4I.
- (a) In conjunction with J3IM and J6, plan JF Information Plan (IMP) and C4I architecture.
 - 1 Develop JF Information system protection (INFOSEC) plan.
 - 2 Develop JF Computer Security (COMPUSEC) plan.
 - 3 Coordinate with J3IW EW officer on EW Electronic protection (EP) plan.



(b) In conjunction with J3IM, J6IM, and J2CI (Counterintelligence), develop JF information, C2 and C4I attack detection process.

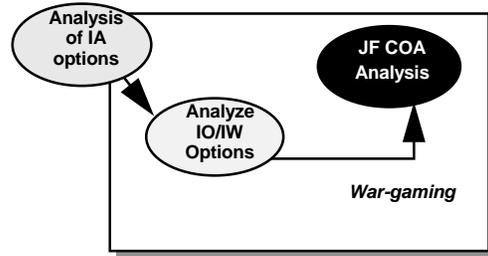
4. **Participate in COA analysis (war gaming).** Be prepared to contribute to the process of war-gaming by mentally “fighting the battle” in time and space. The process may use the structure of action-reaction-counteraction sequences for critical events (e.g., D-Day actions). Analyze IA concepts; war game within the context of other IW operations COAs and the overall JF operational COA (actual COAs developed by operational planners may provide basis for IA COAs). Determine:



- More specific forces required.
- More specific assets/resources required.
- Possible branches (what if) and sequels (what then) to military IA requirements.
- Assess military IA risks.
- Unintended effects.
- Provide input to Time-Phased Force and Deployment Data (TPFDD) development to facilitate execution of IA plan in accordance with the overall JF plan.

5. **Participate in COA comparison.**

- a. Participate in determining the criteria for comparing COAs. Criteria for IA operations could come from:

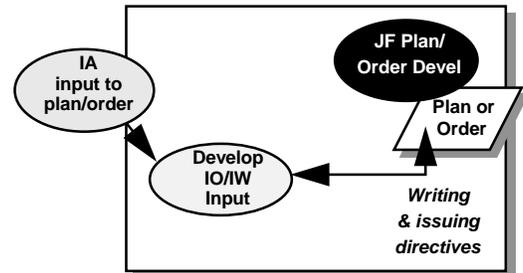


- Commander's Intent
- Factors of METT-T
 - Mission accomplishment
 - Adversary
 - Terrain
 - Troops available
 - Time available

- b. Ensure recommendations for IA operations have been coordinated with the components of the JF.

6. **Receive CJF's decision on COAs.** The CJF may select or modify the recommended COA. Based on that decision, the Commander's Estimate document (or slides) will normally be sent/briefed to the CC for approval.

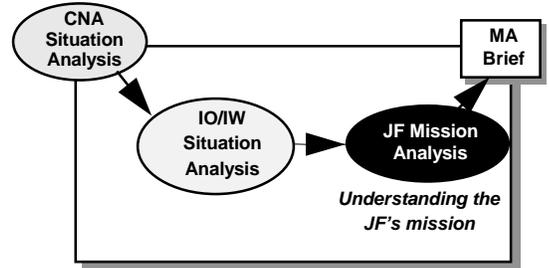
7. **Provide input/develop IA perspective in JF plan/order.** After the COA is selected, the plan/order is physically developed. Most of the information needed for this task should have already been developed through the estimate process (mission analysis through COA selection). IA operations input can be in many sections of the plan/order, however, the primary areas for writing IA operations information are found in Tab G (Defensive Information Operations) to Appendix 3 (Information Operations) to Annex C (Operations) per JOPES (see CJCSM 3122.03).



Appendix 7 – Computer Network Attack

1. Contribute to JF's overall mission analysis

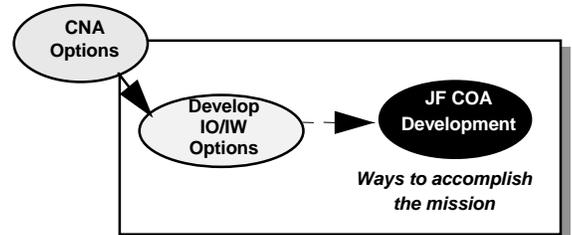
- a. Determine known facts, current status, or conditions of joint forces capable of CNA.
- b. In coordination with the J2, conduct analysis of the adversary.
 - (1) Determine adversary dependence on use of the electromagnetic spectrum.
 - (2) Determine adversary communications attack and CNA capability.
 - (3) Determine Hostile Intelligence System (HOIS) collection capability (see deception and OPSEC mission analysis).
 - (4) Analyze friendly C2 and C4I for vulnerabilities related to use of the CNA and communications attack (see IA mission analysis).
- c. Develop assumptions to replace missing or unknown facts concerning CNA.
- d. Analyze CC's mission and intent from a CNA perspective.
- e. Determine CNA operations limitations.
 - (1) Things CNA must do (constraints).
 - (2) Things CNA cannot do (restraints).
 - (3) Others (e.g., political, legal, diplomatic, etc.).
- f. Determine adversary and own center(s) of gravity (COGs) and tentative decisive points.
 - (1) Determine approaches to adversary COGs.
 - (2) Determine ways to assist in protecting friendly force COGs.
- g. Identify tasks to be performed by CNA.
 - (1) Determine specified CNA tasks.
 - (2) Determine implied CNA tasks.
 - (3) From (1) and (2) above, determine essential CNA tasks or goals.
- h. Conduct initial JF CNA force structure analysis to determine if sufficient assets are available to do the tasks.
- i. Conduct an initial CNA risk assessment. Review risk assessment done by the entire JPG.
- j. Determine end state from a CNA perspective.
- k. Assist in development of JF mission statement.
- l. Assist in development of mission analysis briefing for the CJF.



2. Receive CJF planning guidance. CJF should provide guidance at this point. Planning guidance should be disseminated to IO/IW Cell personnel and the components. If needed, ask the CJF for any guidance necessary for continued planning.

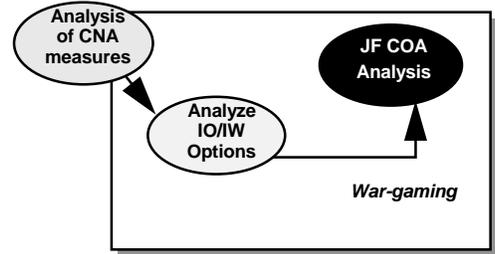
3. Develop CNA options to support the JF's COAs. The JF staff should now develop multiple friendly COAs.

- a. Develop CNA options for initial JF COAs.
 - (1) Review mission analysis and CJF's guidance.
 - (2) Develop CNA options to support the JF's COAs.
 - (a) Plan CNA in support of IW-O.
 - 1 Plan CNA against selected adversary networks; target C2, intelligence, logistics as required to influence the adversary in the desired direction.
 - 2 In conjunction with the J2, develop feedback on CNA operations.

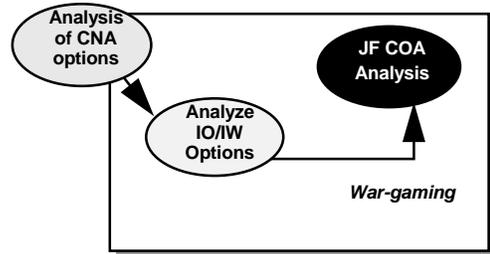


- (b) Plan CNA for protection of friendly C2 and C4I. Integrate CNA with other IW elements to preclude disruption of JF information, C2 and C4I.
 - 1 Plan CNA operations against adversary IW-O capabilities to preclude attacks on friendly information, C2 and C4I.
 - 2 Coordinate with J2 for feedback on active defense operations.

4. **Participate in COA analysis (war gaming).** Be prepared to contribute to the process of war-gaming by mentally “fighting the battle” in time and space. The process may use the structure of action-reaction-counteraction sequences for critical events (e.g., D-Day actions). Analyze CNA concepts. War game within context of other IW operations COAs and the overall JF operational COA (actual COAs developed by operational planners may provide basis for CNA COAs). Determine:
- a. More specific forces required.
 - b. More specific assets/resources required.
 - c. Possible branches (what if) and sequels (what then) to military CNA requirements.
 - d. Assess military CNA risks.
 - e. Unintended effects.
 - f. Provide input to Time-Phased Force and Deployment Data (TPFDD) development to facilitate execution of CNA plan in accordance with the overall JF plan.

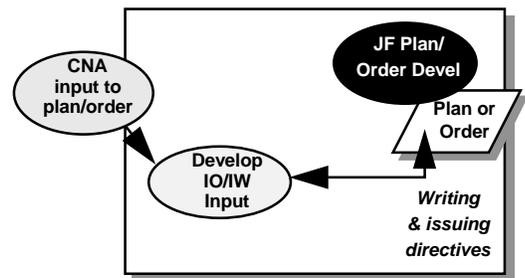


5. **Participate in COA comparison.**
- a. Participate in determining the criteria for comparing COAs. Criteria for CNA operations could come from:
 - (1) Commander's Intent
 - (2) Factors of METT-T
 - (a) Mission accomplishment
 - (b) Adversary
 - (c) Terrain
 - (d) Troops available
 - (e) Time available
 - b. Ensure recommendations for CNA operations have been coordinated with the components of the JF.



6. **Receive CJF's decision on COAs.** The CJF may select or modify the recommended COA. Based on that decision, the Commander's Estimate document (or slides) will normally be sent/briefed to the CC for approval.

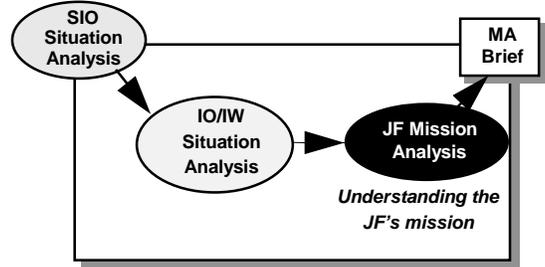
7. **Provide input/develop CNA perspective in JF plan/order.** After the COA is selected, the plan/order is physically developed. Most of the information needed for this task should have already been developed through the estimate process (mission analysis through COA selection). CNA operations input can be in many sections of the plan/order, however, the primary areas for writing CNA information are found in JOPES (see CJCSM 3122.03):
- a. Paragraph 3 (Execution) of Appendix 3 (Information Operations) to Annex C (Operations).
 - b. Tab F (CNA) to Appendix 3 to Annex C.



Appendix 8 – Special Information Operations

1. Contribute to JF's overall mission analysis

- a. Determine known facts, current status, or conditions of joint forces capable of Special Information Operations (SIO).
- b. In coordination with the J2, conduct analysis of the adversary.
- c. Develop assumptions to replace missing or unknown facts concerning SIO.
- d. Analyze CC's mission and intent from an SIO perspective.
- e. Determine operations limitations.
 - (1) Things SIO must do (constraints).
 - (2) Things SIO cannot do (restraints).
 - (3) Others (e.g., political, weather, terrain, etc.).
- f. Determine adversary/ own centers of gravity (COGs) and tentative decisive points.
 - (1) Determine approaches to adversary COGs.
 - (2) Determine ways SIO can assist in protecting friendly force COGs.
- g. Identify tasks to be performed by SIO.
 - (1) Determine specified SIO tasks.
 - (2) Determine implied SIO tasks.
 - (3) From (1) and (2) above, determine essential SIO tasks or goals.
- h. Conduct initial JF SIO force structure analysis to determine if sufficient assets are available to do the tasks.
- i. Conduct an initial SIO risk assessment. Review risk assessment done by the entire JPG.
- j. Determine end state from an SIO perspective.
- k. Assist in development of JF mission statement.
- l. Assist in development of mission analysis briefing for the CJF.



2. Receive CJF planning guidance. CJF should provide guidance. Planning guidance should be disseminated to IO Cell personnel and the components. If needed, ask the CJF for any guidance necessary for continued planning.

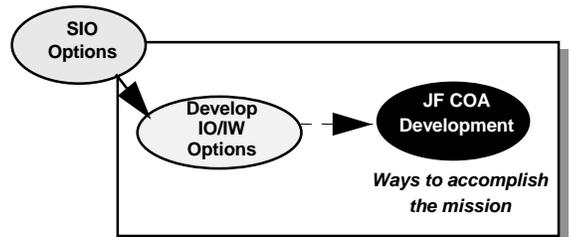
3. Develop SIO options to support the JF's COAs. The JF staff should now develop multiple friendly COAs. Develop SIO options for initial JF COAs.

- a. Review mission analysis and CJF's guidance.
- b. Develop SIO options to support the JF's COAs.

4. Participate in COA analysis (war gaming). Be prepared to contribute to the process of war-gaming by mentally "fighting the battle" in time and space. The process may use the structure of action-reaction-counteraction" sequences for critical events (e.g. D-Day actions).

Analyze SIO concepts. War game within context of other IW operations COAs and the overall JF operational COA (actual COAs developed by operational planners may provide basis for SIO COAs). Determine:

- a. More specific forces required.
- b. More specific assets/resources required.
- c. Possible branches (what if) and sequels (what then) to SIO requirements.
- d. Assess military risks.
- e. Unintended effects.



- f. Provide input to Time-Phased Force and Deployment Data (TPFDD) development to facilitate execution of SIO plan in accordance with the overall JF plan.

5. **Participate in COA comparison**

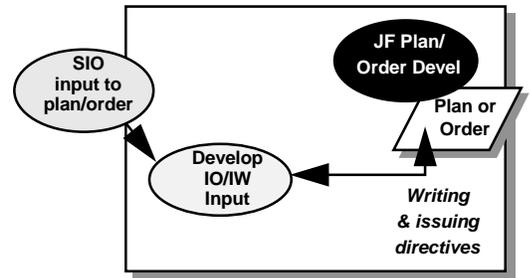
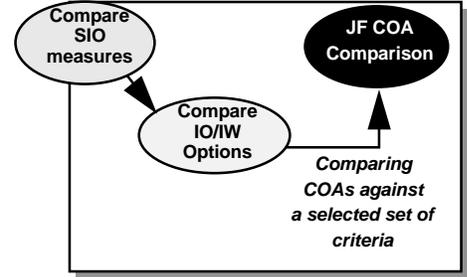
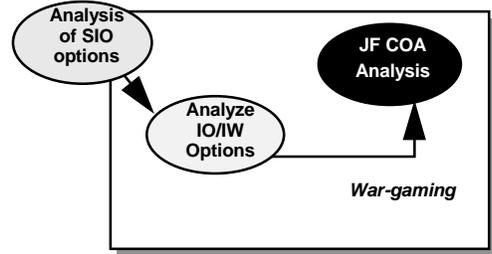
- a. Participate in determining the criteria for comparing COAs. Criteria for SIO could come from:

- (1) Commander's Intent
- (2) Factors of METT-T
 - (a) Mission accomplishment
 - (b) Adversary
 - (c) Terrain
 - (d) Troops available
 - (e) Time available

- b. Ensure recommendations for SIO have been coordinated with the components of the JF.

6. **Receive CJF's decision on COAs.** The CJF may select or modify the recommended COA. Based on that decision, the Commander's Estimate document (or slides) will normally be sent/briefed to the CC for approval.

7. **Provide input/develop SIO perspective in JF plan/order.** After the COA is selected, the plan/order is physically developed. Most of the information needed for this task should have already been developed through the estimate process (mission analysis through COA selection). SIO input can be found in a separate classified Annex S (STO) per JOPES (see CJCSM 3122.03).



Annex B – Glossary

Abbreviations and Acronyms

Abbreviation / Acronym	Definition
AADC	Area Air Defense Commander
AAV	Amphibious Assault Vehicle
ACA	Airspace Control Authority
ACE	Air Control Element
AD	Air Defense
ADA	Air Defense Area
ADCON	Administrative Control
AFB	Air Force Base
AFFOR	Air Force Forces
AFS	Air Force Squadron
AFSOF	Air Force Special Operations Forces
AFIWC	Air Force Information Warfare Center
AIA	Air Intelligence Agency
AIS	Automated Information Systems
ALO	Air Liaison Officer
ALSA	Air, Land, Sea Operations
AMC	U.S. Air Mobility Command
AME	Air Mobility Element
Amph	Amphibious
AO	Area of Operations
AOR	Area of Responsibility
APC	Armored Personnel Carrier
APOD	Aerial Port of Debarkation
APOE	Aerial Port of Embarkation
ARCENT	Army Forces Central Command
ARFOR	Army Forces
ARG	Amphibious Ready Group
ARSOF	Army Special Operations Forces
ASD(C3I)	Assistant Secretary of Defense for Command, Control, Communications and Intelligence
ASD(PA)	Assistant Secretary of Defense for Public Affairs
ASD(SOLIC)	Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict
ATACMS	Army Tactical Missile System
ATF	Amphibious Task Force
ATM	Asynchronous Transfer Mode
ATO	Air Tasking Order
AVN	Aviation
BCD	Battlefield Coordination Detachment
BDA	Battle Damage Assessment
Bde	Brigade
BLT	Battalion Landing Team

Joint Information Operations Planning Handbook – July 2003

Abbreviation / Acronym	Definition
BIOSG	Bilateral Information Operations Steering Group
BIOWG	Bilateral Information Operations Working Group
Bn	Battalion
BPT	Be Prepared To
CC	Combatant Commander; Combatant Command
C2	Command and Control
C2W	Command and Control Warfare
C4I	Command, Control, Communications, Computers, and Intelligence
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance
CA	Civil Affairs
CAAP	Critical Asset Assurance Program
CALCM	Conventional Air Launched Cruise Missile
CAG	Civil Affairs Group
CAP	Crisis Action Planning
CAS	Close Air Support
CCIR	Commander's Critical Information Requirements
CCS	Command and Control Squadron
CD	Civil Defense; Counter Deception
C-Day	Unnamed day on which a deployment operation begins
CDCM	Coastal Defense Cruise Missile
Cdr	Commander
CENTCOM	U.S. Central Command
CERT	Computer Emergency Response Team
CEP	Circular Error Probability
CFACC	Combined Force Air Component Commander
CFC	Combined Forces Command (Korea)
CFH	Contingency Forward Headquarters
CFLCC	Combined Force Land Component Commander
CFMCC	Combined Force Maritime Component Commander
CFSOTF	Combined Forces Special Operations Task Force
CG	Cruiser, Guided Missile
CHE	Cargo or Container Handling Equipment
CI	Counterintelligence
CIA	Central Intelligence Agency
CIAO	Critical Infrastructure Assurance Office
CINC	Commander-in-Chief (generally referred to as Combatant Commander)
CIP	Critical Infrastructure Protection
CIPIS	Critical Infrastructure Protection Integration Staff
CIPWG	CIP Working Group
CIRT	Computer Incident Response Team
CIS	Communications and Information Systems
CISO	Counterintelligence Support Officer
CITAC	Computer Investigation and Infrastructure Threat Center
Civ	Civilian
Civ-Mil	Civilian-Military
CJCS	Chairman of the Joint Chiefs of Staff

Joint Information Operations Planning Handbook – July 2003

Abbreviation / Acronym	Definition
CJCSM	Chairman, Joint Chiefs of Staff Manual
CJTF	Commander, Joint Task Force (U.S.); Combined Joint Task Force (NATO)
CM	Consequence Management
CMO	Civil-Military Operations
CMOC	Civil-Military Operations Center; Civil-Military Operations Cell
CNA	Computer Network Attack
CND	Computer Network Defense
CNE	Computer Network Exploitation
CNN	Cable News Network
CNR	Computer Network Reconnaissance
COA	Course of Action
COCOM	Combatant Command
COG	Center of Gravity
COLISEUM	Community On-Line Intelligence System for End-Users and Managers
COMCARGRU	Commander, Carrier Group
COMDESRON	Commander, Destroyer Squadron
Comm	Communications
COMSEC	Communications Security
COMM Z	Communication Zone
CONOPS	Concept of Operations
CONPLAN	Concept Plan
COP	Common Operational Picture
CoS	Chief of Staff
COSCOM	Corps Support Command
CPG	Contingency Planning Guidance
CSA	Chief of Staff, U.S. Army
CSAR	Combat Search and Rescue
CSC	Combatant Commander's Strategic Concept
CSS	Combat Service Support
CSSA	Combat Service Support Area
CSSE	Combat Service Support Element (of MAGTF)
CVBG	Aircraft Carrier Battle Group
CVN	Aircraft Carrier (Nuclear Powered)
CVW	Aircraft Carrier Air Wing
CW	Chemical Warfare
CWO	Communications Watch Officer
DA	Direct Action
DAL	Defended Asset List
DARSS	Daily Airborne Reconnaissance and Surveillance Syndicate
DART	Disaster Assistance Response Team
DASD S&IO	Deputy Assistant Secretary of Defense for Security and Information Operations
DAT	Defense Attaché
DC	Deputies Committee
DCI	Director of Central Intelligence
DCJTF	Deputy Commander, Joint Task Force
DCM	Deputy Chief of Mission

Joint Information Operations Planning Handbook – July 2003

Abbreviation / Acronym	Definition
DD	Destroyer
D-Day	Day on which operations commence or are scheduled to commence
DDG	Destroyer, Guided Missile
DDIO	Deputy Director for Information Operations (U.S. Joint Staff)
DDO	Director of Operations
DepCJTF	Deputy Commander, Joint Task Force
DIA	Defense Intelligence Agency
DIAP	Defense-Wide Information Assurance Program
DIAPSG	Defense-Wide Information Assurance Program Steering Group
DII	Defense Information Infrastructure
DIOC	Defense Information Operations Council
DIRLAUTH	Direct Liaison Authorized
DIRMOBFOR	Director of Mobility Forces
DIRNSA	Director, National Security Agency
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
Div	Division
DJTFAAC	Deployable Joint Task Force Augmentation Cell
DLA	Defense Logistics Agency
DoC	Department of Commerce
DOCC	Deep Operation Coordination Cell
DoD	Department of Defense
DoDIP	DoD Intelligence Plan
DoE	Department of Energy
DoJ	Department of Justice
DoS	Department of State
DP	Displaced Person
DPRE	Displaced Person / Refugee
DTRA	Defense Transportation Regulation; Defense Threat Reduction Agency
EA	Electronic Attack
EOA	Enemy Course of Action
ECS	Electronic Combat Squadron
EEFI	Essential Elements of Friendly Information
ELINT	Electronic Intelligence
EP	Electronic Protection
ES	Electronic Support
EUCOM	U.S. European Command
EW	Electronic Warfare; Early Warning
F2C2	Friendly Force Coordination Center or Cell
FBI	Federal Bureau of Investigation
FDO	Flexible Deterrent Option
FEDCIRC	Federal Computer Incident Response Capability
FEMA	Federal Emergency Management Agency
FFG	Frigate, Guided Missile
FFIR	Friendly Force Information Requirements
FID	Foreign Internal Defense

Joint Information Operations Planning Handbook – July 2003

Abbreviation / Acronym	Definition
FIE	Fly-In Echelon
FIRST	Forum of Incident Response and Security Teams
FISINT	Foreign Instrumentation Signals Intelligence
FIWC	Fleet Information Warfare Center
FLOT	Forward Line of Own Troops
FOB	Forward Operations Base
FP	Force Protection
FPWG	Force Protection Working Group
FRAGO, FRAGORD	Fragmentary Order
FS	Fighter Squadron
FSB	Forward Staging Base
FSCL	Fire Support Coordination Line
FSCM	Fire Support Coordination Measure
FSE	Fire Support Element
FSSG	Force Service Support Group (of MAGTF)
FUNCPLAN	Functional Plan
FW	Fighter Wing
G-2	Army or Marine Corps Component Intelligence Staff Officer
G-3	Army or Marine Corps Component Operations Staff Officer
GAT	Guidance, Apportionment, and Targeting
GCC	Gulf Coordination Council
GCCS	Global Command and Control System
GNOSC	Global Network Operations Security Center
GPS	Global Positioning System
GTN	Global Transportation Network
GSA	General Services Administration
HA	Humanitarian Assistance
HACC	Humanitarian Action Coordination Center
HAST	Humanitarian Assistance Survey Team
HCA	Humanitarian and Civic Assistance
HET	Heavy Equipment Transporter
HLD	Homeland Defense
HLS	Homeland Security
HN	Host Nation
HNS	Host Nation Support
HUMINT	Human Intelligence
IA	Interagency; Information Assurance
IADS	Integrated Air Defense System
IATAC	Information Assurance Technology Analysis Center
IAW	In Accordance With
IC	Intelligence Community
ICC	Information Coordination Center
ICE	Interdiction Control Element
ICSB	Intelligence Collection Synchronization Board; Interim Command Switch Board
IM	Information Management
IMINT	Imagery Intelligence

Joint Information Operations Planning Handbook – July 2003

Abbreviation / Acronym	Definition
IMI	International Military Information
IMO	Information Management Officer
Info	Information
INFOCON	Information Condition
INMARSAT	International Maritime Satellite
INR	Bureau of Intelligence and Research (DoS)
IO	Information Operations; International Organization
ION	Information Operations Navigator
IO S&I	Information Operations Strategy and Integration
IOSS	Interagency OPSEC Support Staff
IOTC	Information Operations Technology Center
IOTF	Information Operations Task Force
IOWG	Information Operations Working Group
IPB	Intelligence Preparation of the Battlespace
IPI	International Public Information
IPTF	Infrastructure Protection Task Force
ISB	Intermediate Staging Base
ISR	Intelligence, Surveillance, and Reconnaissance
IW	Information Warfare
IWSC	Information Warfare Support Center
JAC	Joint Analysis Center
JAG	Judge Advocate General
JAOC	Joint Air Operations Center
JCB	Joint Coordination Board
JCCC	Joint Communications Control Center
JCIWS	Joint Command, Control, and Information Warfare School
JCMA	Joint COMSEC (Communications Security) Monitoring Activity
JCMOTF	Joint Civil-Military Operations Task Force
JCS	Joint Chiefs of Staff
JCSE	Joint Communications Support Element
JDISS	Joint Deployable Intelligence Support System
JDLC	Joint Distributed Learning Center
JDOC	Joint Defense Operations Center
JF	Joint Force
JFACC	Joint Force Air Component Commander
JFAST	Joint Flow and Analysis System for Transportation
JFC	Joint Force Commander
JFCOM	U.S. Joint Forces Command
JFSC	Joint Forces Staff College
JFE	Joint Fires Element
JFHQ	Joint Forces Headquarters (UK)
JFLCC	Joint Force Land Component Commander
JFMCC	Joint Force Maritime Component Commander
JFSOCC	Joint Force Special Operations Component Commander
JGAT	Joint Guidance, Apportionment, and Targeting (Cell)
JIB	Joint Information Bureau

Joint Information Operations Planning Handbook – July 2003

Abbreviation / Acronym	Definition
JIC	Joint Intelligence Center
JICO	Joint Interface Control Officer
JIMB	Joint Information Management Board
JIOC	Joint Information Operations Center
JIOPC	Joint Information Operations Planning Course
JIPB	Joint Intelligence Preparation of the Battlespace
JIPTL	Joint Integrated Prioritized Target List
JISE	Joint Intelligence Support Element
JITC	Joint Interoperability Test Command
JIVA	Joint Intelligence Virtual Architecture
JIWSOC	Joint Information Warfare Staff and Operations Course
JLRC	Joint Logistics Readiness Center
JMC	Joint Movement Center
JMD	Joint Manning Document
JMETL	Joint Mission Essential Task List
JOA	Joint Operations Area
JOC	Joint Operations Center
JOPES	Joint Operation Planning and Execution System
JP	Joint Publication
JPEC	Joint Planning and Execution Community
JPG	Joint Planning Group
JPO-STC	Joint Program Office for Special Technology Countermeasures
JPOTF	Joint Psychological Operations Task Force
JPRA	Joint Personnel Recovery Agency
JPRC	Joint Personnel Reception Center
JRA	Joint Rear Area
JRAC	Joint Rear Area Coordinator
JRFL	Joint Restricted Frequency List
JRSOI	Joint Reception, Staging, Onward Movement, and Integration
JRVIO	Joint Reserve Virtual Information Operations
JS	Joint Staff
JSC	Joint Spectrum Center
JSOA	Joint Special Operations Area
JSOTF	Joint Special Operations Task Force
JSCP	Joint Strategic Capabilities Plan
JSRC	Joint Search and Rescue Center
JSTARS	Joint Surveillance and Targeting Attack Radar System
JTASC	Joint Training, Analysis and Simulation Center
JTAV	Joint Total Asset Visibility
JTB	Joint Transportation Board
JTCB	Joint Targeting Coordination Board
JTF	Joint Task Force
JTF-CNO	Joint Task Force for Computer Network Operations
JTSG	Joint Targeting Steering Group
JTTP	Joint Tactics, Techniques, and Procedures
JVB	Joint Visitors Bureau

Joint Information Operations Planning Handbook – July 2003

Abbreviation / Acronym	Definition
JWAC	Joint Warfare Analysis Center
JWFC	Joint Warfighting Center
JWICS	Joint Worldwide Intelligence Communications System
LAN	Local Area Network
LCC	Land Component Commander; Launch Control Center
LHA	Amphibious Assault Ship (General Purpose)
LHD	Amphibious Assault Ship (Multi-Purpose)
LIWA	Land Information Warfare Activity (now the 1 st Information Operations Command [Land])
LNO	Liaison Officer
LOC	Line of Communication; Logistics Operations Center
LPD	Amphibious Transport Dock
LRC	Logistics Readiness Center
LRPE	Long Range Planning Element
LSD	Landing Ship Dock
MAAP	Master Air Attack Plan
MACG	Marine Air Control Group
MAG	Marine Air Group
MAGTF	Marine Air, Ground Task Force
MARFOR	Marine Forces
MARLO	Marine Liaison Officer
MASINT	Measurement and Signature Intelligence
MAW	Marine Air Wing
MB	Megabytes
MCM	Mine Countermeasures Ship
MCMRON	Mine Countermeasures Squadron
MEB	Marine Expeditionary Brigade
MEF	Marine Expeditionary Force
METT-TC	Mission, Enemy, Terrain, Troops, Time Available, and Civilians
MEU	Marine Expeditionary Unit
MHE	Materials Handling Equipment
MI	Military Intelligence
MINERVA	Military Information Nexus Enabling Relevant and Valid Analysis
MIO	Maritime Interdiction Operations
MOE	Measure of Effectiveness
MOG	Maximum (aircraft) on the Ground
MOOTW	Military Operations Other Than War
MPSRON	Maritime Patrol Squadron; Maritime Pre-positioned Ship Squadron
MSCA	Military Support to Civil Authorities
MSR	Main Supply Route
MTG	Master Training Guide
MWSG	Marine Wing Support Group
NAF	Numbered Air Force
NALE	Naval Amphibious Liaison Element
NATO	North Atlantic Treaty Organization
NAVFOR	Navy Forces
NAVSO	Navy Special Operations Forces

Joint Information Operations Planning Handbook – July 2003

Abbreviation / Acronym	Definition
NBC	Nuclear, Biological, Chemical
NCA	National Command Authorities (use POTUS or SECDEF)
NCOIC	Noncommissioned Officer-in-Charge
NCS	National Communications Systems
NCTF-CND	Navy Component Task Force for Computer Network Defense
NEO	Noncombatant Evacuation Operations
NGO	Non-Governmental Organization
NIAP	National Infrastructure Assurance Partnership
NIPC	National Infrastructure Protection Center
NIST	National Intelligence Support Team
NIWA	Naval Information Warfare Activity
NORTHCOM	U.S. Northern Command
NOSC	Network Operations Security Center
NSA	National Security Agency
NSC	National Security Council
NSIRC	National Security Incident Response Center
NSOC / IPC	National Security Operations Center / Information Protect Cell
NSPD	National Security Presidential Directive
NSS	National Security Strategy
NSTAC	National Security Telecommunications Advisory Committee
NSTC	National Science and Technology Council
NSTISSC	National Security Telecommunications and Information Systems Security Council
NSWTG	Navy Special Warfare Task Group
NTIA	National Telecommunications and Information Assurance
NWAG	Naval Warfare Analysis Group
OAF	Operation ALLIED FORCE
OEF	Operation ENDURING FREEDOM
OFDA	Office of Foreign Disaster Assistance
OGA	Other Government Agencies
OJE	Operation JOINT ENDEAVOR
OMB	Office of Management and Budget
ONDCP	Office of National Drug Control Policy
OODA	Observe Orient Decide Act
OOTW	Operations Other Than War
OPCEN	Operations Center
OPCON	Operational Control
OPE	Operations Planning Element
OPEC	Organization of Petroleum Exporting Countries
OPFOR	Opposition Force
OPG	Operations Planning Groups
OPLAN	Operations Plan
OPORD	Operations Order
OPR	Office of Primary Responsibility
OPSEC	Operations Security
OPT	Operations Planning Team
OPTASK	Operational Tasking Order

Joint Information Operations Planning Handbook – July 2003

Abbreviation / Acronym	Definition
OPTEMPO	Operational Tempo
OSD	Office of the Secretary of Defense
OSINT	Open Source Intelligence
OSTP	Office of Science and Technology Policy
PA	Public Affairs
PACOM	U.S. Pacific Command
PAO	Public Affairs Officer
PC	Patrol Craft; Principles Committee
PCAST	President's Committee of Advisors on Science and Technology
PCC	Policy Coordination Committee
PCCIP	President's Commission on Critical Infrastructure Protection
PD	Public Diplomacy
PDD	Presidential Decision Directive
PfP	Partnership for Peace
PID	Plan Identification Number
PIR	Priority Intelligence Requirements
PJHQ	Peacetime Joint Headquarters (UK)
PMO	Program Management Office
POAS	PSYOP Automated System
POD	Port of Debarkation
POE	Port of Embarkation
POG	Psychological Operations Group
POLAD	Political Advisor
POTF	Psychological Operations Task Force
POTUS	President of the United States
POW	Prisoner of War
PPBS	Planning, Programming, and Budgeting System
PR	Personnel Recovery; Public Relations
PSYOP	Psychological Operations
PTG	Patrol Boat Guided Missile
Pub	Publication
PVO	Private Voluntary Organization (replaced by NGO)
PWRMS	Prepositioned War Reserve Material Stocks
R & D	Research and Development
RCC	Rescue Coordination Center
RFI	Request for Information
RPP	Regional Program Plan
ROE	Rules of Engagement
RW	Reconnaissance Wing; Rotary Wing
SA	Situational Awareness
SAG	Surface Action Group
SAP	Special Access Program
SAR	Search and Rescue
SAT	Situational Assessment Team; Satellite
SATCOM	Satellite Communications; Satellite Command
SEAD	Suppression of Enemy Air Defenses

Joint Information Operations Planning Handbook – July 2003

Abbreviation / Acronym	Definition
SEAL	Sea–Air–Land (team)
SECDEF	Secretary of Defense
SERE	Survival, Evasion, Resistance, Escape
SHORAD	Short Range Air Defense
SIGINT	Signals Intelligence
SIO	Special Information Operations
SITREP	Situation Report
SJA	Staff Judge-Advocate
SLAM	Stand-off Land Attack Missile
SLOC	Surface Line of Communication
SOAR	Special Operations Aviation Regiment
SOC	Special Operations Command
SOCOM	U.S. Special Operations Command
SOF	Special Operations Force
SOFA	Status of Forces Agreement
SOLE	Special Operations Liaison Element
SOP	Standing Operating Procedures
SOUTHCOM	U.S. Southern Command
SPACECOM	U.S. Space Command (disestablished)
SPECOPS	Special Operations
SPOD	Sea Port of Debarkation
SPOE	Sea Port of Embarkation
SR	Special Reconnaissance
SRIG	Surveillance, Reconnaissance, and Intelligence Group
SROE	Standing Rules of Engagement
SSM	Surface-to-Surface Missile
SSN	Attack Submarine (Nuclear)
STO	Special Technical Operations
STRATCOM	U.S. Strategic Command
STU	Secure Telephone Unit
TAA	Tactical Assembly Area
TACAIR	Tactical Air
TACON	Tactical Control
TACSAT	Tactical Satellite
TALCE	Tactical Air Lift Control Element
TCF	Tactical Combat Force
TECHINT	Technical Intelligence
TEL	Transporter/Erector/Launcher
TEP	Theater Engagement Plan (replaced by TSCP)
TLAM	Tomahawk Land-Attack Missile
TMD	Theatre Missile Defense
TPFDD	Time-Phased Force and Deployment Data
TRANSCOM	U.S. Transportation Command
TRAP	Tactical Recovery of Aircraft and Personnel
TSCP	Theater Security Cooperation Plan
TST	Time-Sensitive Target

Joint Information Operations Planning Handbook – July 2003

Abbreviation / Acronym	Definition
TV	Television
TWI	Transnational Warfare Interests
UAV	Unmanned Aerial Vehicle
UCCE	Unintended Civilian Casualty Estimate
UCP	Unified Command Plan
UJTL	Universal Joint Task List
ULN	Unit Line Number
UN	United Nations
USAID	United States Agency for International Development
USD(P)	Under Secretary of Defense for Policy
USG	United States Government
USTR	United States Trade Representative
UTC	Unit Type Code
VP	Maritime Control Squadron
VTC	Video Teleconference
WARNORD	Warning Order
WMD	Weapons of Mass Destruction

Joint Publication References

Although numerous Joint Publications provide additional information on the topics presented in this Handbook, the following publications provide the majority of information on Information Operations and are recommended for review.

Joint Publications:

	Joint Doctrine Capstone and Keystone Primer
0-2	Unified Action Armed Forces (UNAAF)
1	Joint Warfare
1-0	Doctrine for Personnel Support to Joint Operations
2-0	Joint Doctrine for Intelligence Support to Operations
2-01.1	Joint Tactics, Techniques, and Procedures for Intelligence Support to Targeting
2-01.3	Joint Tactics, Techniques, and Procedures for Joint Intelligence Preparation of the Battlespace (JIPB)
3-0	Doctrine for Joint Operations
3-13	Joint Doctrine for Information Operations
3-33	Joint Force Capabilities
3-35	Joint Deployment and Redeployment Doctrine
3-51	Joint Doctrine for Electronic Warfare
3-53	Doctrine for Joint Psychological Operations
3-54	Joint Doctrine for Operations Security
3-56	Command and Control Doctrine for Joint Operations
3-57	Doctrine for Joint Civil Affairs
3-58	Joint Doctrine for Military Deception
3-60	Doctrine for Joint Targeting
3-61	Doctrine for Public Affairs in Joint Operations
3-56.1	Command and Control for Joint Air Operations
4-0	Doctrine for Logistic Support of Joint Operations
4-01.8	Joint Reception, Staging, On-ward Movement and Integration Doctrine
5-0	Doctrine for Planning Joint Operations
5-00.2	Joint Task Force Planning Guidance and Procedures

Joint Publications:

6-0	Doctrine for Command, Control, Communications, and Computer (C4) Systems Support to Joint Operations
-----	--

CJCS Manuals:

3122.01	Joint Operation Planning and Execution System (JOPES), Volume I, Planning Policies and Procedures
3122.02	Joint Operation Planning and Execution System (JOPES), Volume III, Crisis Action Time-Phased Force and Deployment Data Development and Deployment Execution
3122.03	Joint Operation Planning and Execution System (JOPES), Volume II, Planning Formats and Guidance
3500.05	Joint Task Force Headquarters Master Training Guide (JTF HQ MTG)

Joint Publication Availability

The above publications may be obtained through several sources:

- Joint Electronic Library - Either CD-ROM from the Joint Warfighting Center, Doctrine Division, in Portsmouth, VA or online at <http://www.jwfc.js.smil.mil/>
- DTIC Website (available in Adobe Acrobat .pdf format): <http://www.dtic.mil/doctrine/>

Match IO Effects Words with IO Capabilities and Related Activities

This table was created by scanning JP 3-13 for usage of various “effects” words (verbs). A “D” in the table means that the effect is referenced by doctrine; “S” means there is a suggested reference based on current usage. The JCIWS faculty uses this technique to easily match a desired IO effect with doctrinal IO capabilities and related activities.

	Convince	Defend	Degrade	Deny	Destroy	Diminish	Disrupt	Exploit	Expose	Influence	Inform	Mislead	Negate	Neutralize	Prevent	Protect	Safeguard	Shape
Civil Affairs								D		D	S							
CNA			D	D	D		D											
CND		S		S											S	S	S	
Counter-deception						D		S					D	D				
Counterintelligence		D														D		
Counter-propaganda								D										
Destruction					D													
Electronic Warfare			D	D	D		D	D		D				D		D		
Information Assurance		D		D												D	S	
INFOSEC		D		D												D		
Military Deception	S									D		D						
OPSEC				D												S		
Physical Security															D		D	
PSYOP	S									D								D
Public Affairs	S									S	D							S

IO Effects Definitions

The JCIWS faculty has found it convenient to gather a set of both doctrinal and non-doctrinal definitions of terms for IO effects we wish to achieve.

Convince	<ul style="list-style-type: none"> <input type="checkbox"/> To overcome by argument <input type="checkbox"/> To bring to belief, consent, or a course of action
Degrade	<ul style="list-style-type: none"> <input type="checkbox"/> Damage done to the function is permanent, but only portions of the function were affected; that is, the function still operates, but not fully. <input type="checkbox"/> A function's operation is permanently impaired, but the damage does not extend to all facets of the function's operation.
Deny	<ul style="list-style-type: none"> <input type="checkbox"/> Damage done to the function is only temporary, but all aspects of the function were affected. <input type="checkbox"/> A function's operation is impaired over the short term, but the damage extends to all facets of the function's operation.
Destroy	<ul style="list-style-type: none"> <input type="checkbox"/> Damage done to the function is permanent, and all aspects of the function have been affected. <input type="checkbox"/> A function's operation is permanently impaired, and the damage extends to all facets of the function's operation.
Diminish	<ul style="list-style-type: none"> <input type="checkbox"/> To make less or cause to appear less. <input type="checkbox"/> To reduce the effectiveness of an activity. This is similar to degrade without the kinetic overtones.
Disrupt	<ul style="list-style-type: none"> <input type="checkbox"/> Damage done to the function is temporary, and only portions of the function were affected. <input type="checkbox"/> A function's operation is impaired over the short term and the damage does not extend to all facets of the function's operation.
Exploit	<ul style="list-style-type: none"> <input type="checkbox"/> Attempts to gather information that will enable opposition ability to conduct operations to induce other Effects.
Expose	<ul style="list-style-type: none"> <input type="checkbox"/> To make known or cause to be visible to public view. <input type="checkbox"/> To make visible, to reveal something undesirable or injurious.
Influence	<ul style="list-style-type: none"> <input type="checkbox"/> Selected projection or distortion of the truth to persuade the opposition to act in a manner detrimental to mission accomplishment while benefiting accomplishment of friendly objectives. <input type="checkbox"/> To cause a change in the character, thought, or action of a particular entity.
Inform	<ul style="list-style-type: none"> <input type="checkbox"/> To impart information or knowledge.
Mislead	<ul style="list-style-type: none"> <input type="checkbox"/> Creation of a false perception that leads the opposition to act in a manner detrimental to mission accomplishment while benefiting accomplishment of friendly objectives.
Prevent	<ul style="list-style-type: none"> <input type="checkbox"/> To deprive of hope or power of acting or succeeding. <input type="checkbox"/> To keep from happening, to avert.
Protect Safeguard	<ul style="list-style-type: none"> <input type="checkbox"/> To cover or shield from exposure, damage, or destruction. <input type="checkbox"/> To keep from harm, attack, injury or exploitation. <input type="checkbox"/> To maintain the status or integrity of.
Negate Neutralize	<ul style="list-style-type: none"> <input type="checkbox"/> To render ineffective, invalid or unable to perform a particular task or function. <input type="checkbox"/> To counteract the activity or effect of.
Shape	<ul style="list-style-type: none"> <input type="checkbox"/> To determine or direct the course of events. <input type="checkbox"/> To modify behavior by rewarding changes that tend toward a desired response. <input type="checkbox"/> To cause to conform to a particular form or pattern.