1st IO CMD (Land)
IO Planner's Aid

Key Definitions

Information Operations: (IO) The employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with specified supporting and related capabilities, to affect or defend information and information systems, and to influence decision making. (FM 3-13)

Information Environment: The aggregate of individuals, organizations, or systems that collect, process, or disseminate information; also included is the information itself. (FM 3-0)

Information Superiority: The operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. (FM 3-0)

Updated by EWA IIT (Garry Beavers) November 2003

IO and MDMP

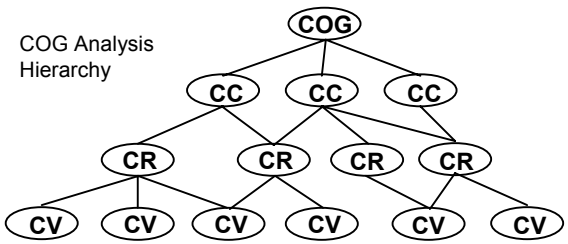
MDMP Step	IO Focus
Receipt of Mission	• Conduct initial assessment of info op • Determine IO planning requirements
Mission Analysis	• Understand IO situation • Analyze HHQ information operation • Define & analyze the info environment and threat • Develop IO mission statement & objectives • Seek commander's IO guidance
COA Development	• ID friendly IO capabilities & vulnerabilities • Develop IO concept of support
COA Analysis	• Visualize operations in the info environment • Wargame IO concept of support against how the enemy will employ its information systems and assets
COA Comparison	• Analyze & evaluate IO support to each COA
COA Approval	• Finalize details of the information operation
Orders Production	• Prepare IO annex & input to base order/plan

Information IPB

IPB Step	IO Focus	Analysis Product
Define the Battlefield	Define the Information Environment	Combined Information Overlay - Significant characteristics of the info environment & effects on operations
Describe the Battlefield's Effects	Describe the Information Environment's Effects	
Evaluate the Threat	Evaluate the Threats' Info System	Threat COG Analysis - Critical vulnerabilities Threat Templates - Who makes decisions; what nodes, links, & systems the threat uses; how info assets are employed
Determine Threat COAs	Determine Threat Actions in the Info Environment	Information SITEMP - When, where, & why the threat will seek to gain info superiority

Centers of Gravity (COG)

COG Analysis Hierarchy



Definitions

Center of Gravity (COG): Primary source of moral or physical strength, power, and resistance.

Critical Capability (CC): Primary abilities which merit a COG to be identified as such in the context of a given scenario, situation, or mission.

Critical Requirement (CR): Essential conditions, resources, and means for a critical capability to be fully operative.

Critical Vulnerability (CV): Critical requirements (or components thereof) which are deficient or vulnerable to attack or influence in a manner achieving decisive results.

COG Analysis Steps

1. Identify potential threat COGs. Visualize the threat as a system of functional components. Based upon how the threat organizes, fights, makes decisions, and its physical and psychological strengths and weaknesses, select the threat's primary source of moral or physical strength, power, and resistance.
2. Identify Critical Capabilities (CC). Each COG is analyzed to determine what primary abilities (functions) the threat possesses in the context of the battlefield and friendly mission that can prevent friendly forces from accomplishing the mission. Each identified CC must relate to the COG, otherwise it is not critical in the context of the analysis.
3. Identify Critical Requirements (CRs) for each CC. A CR is a condition, resource, or means that enables threat functions or mission. CRs are usually tangible elements such as communications means, weapons systems, or even geographical areas or features. There may be more than one CR per CC.
4. Identify Critical Vulnerabilities (CVs) for each CR. A CV is a CR, or component of a CR, which is vulnerable to attack or influence. As the hierarchy of CRs, and CVs are developed, inter-relationships and overlapping between the factors are sought in order to identify CRs and CVs that support more than one CC. When selecting CVs, CV analysis is conducted to pair CVs against friendly capabilities.

Validity Testing for COGs

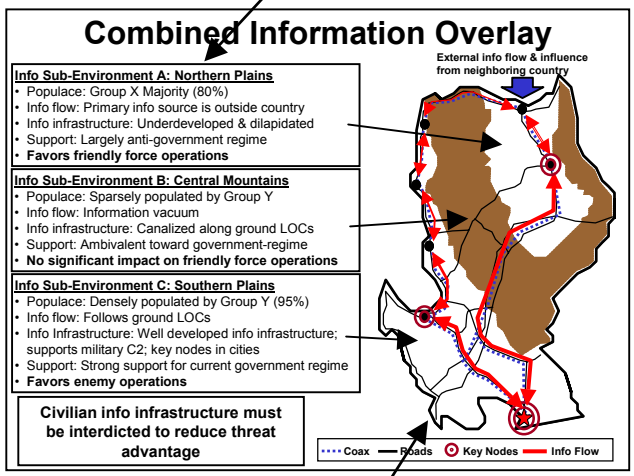
- ✓ Will destruction, neutralization, or substantial weakening of the COG result in changing the threat's COA or denying its objective?
- ✓ Does the friendly force have the resources and capability to accomplish destruction or neutralization of the threat COG? If the answer is "no", then the threat's identified critical factors must be reviewed for other critical vulnerabilities, or planners must reassess how to attack the previously identified critical vulnerabilities with additional resources.

Criteria for CV Analysis (CARVER)

- **C**riticality. An estimate of the CVs importance to the enemy. A vulnerability will significantly influence the enemy's ability to conduct or support operations.
- **A**ccessibility. A determination of whether the CV is accessible to the friendly force in time and place.
- **R**ecuperability. An evaluation of how much effort, time, & resources the enemy must expend if the CV is successfully affected.
- **V**ulnerability. A determination of whether the friendly force has the means or capability to affect the CV.
- **E**ffect. A determination of the extent of the effect achieved if the CV is successfully exploited.
- **R**ecognizability. A determination if the CV, once selected for exploitation, can be identified during the operation by the friendly force, and can be assessed for the impact of the exploitation.

Example Combined Information Overlay

Significant characteristics of each information sub-environment



Graphic portrayal of information environment

Example IO Mission and Objectives

(Tactical Corps mission)

IO Mission: On order, XX Corps IO disrupts 1st Operational Strategic Command (OSC) ground and air defense forces' command and control, influences civilian populace perceptions, and protects Corps' critical information in the AOR in order to facilitate destruction of 1st OSC forces.

IO Objectives:

- Disrupt 1st OSC AD C2 in order to prevent coordinated engagement of XX Corps' deep attacks.
- Destroy 1st OSC headquarters in order to neutralize command and control between battlezone and reserve forces.
- Disrupt operational reserve CPs and communication nets in order to delay employment of reinforcing or counterattack forces.
- Influence civilian populace in occupied areas in order to minimize interference with XX Corps' operations.
- Deny SPF detection and identification of XX Corps' main and tactical CPs in order to prevent targeting by 1st OSC artillery fires.

Defensive IO Effects

EFFECTS	DESCRIPTIVE EXPLANATION
PROTECTION	Actions taken to guard against espionage or capture of sensitive equipment and information.
DETECTION	Discover or discern the existence, presence, or fact of an intrusion into information systems.
RESTORATION	Bring information systems back to their original state.
RESPONSE	React quickly to an adversary's information operations attack or intrusion.

(FM 3-13)

Possible IO Tasks (Non-Doctrinal)

Control	*Inform*
Counter	Interdict
Counter-Recon	Isolate
Defeat	*Jam*
Delay	Neutralize
Demonstrate	*Persuade*
Destroy	*Prevent*
Deter	*Protect*
Engage	Secure
Fix	Suppress

Note: Italicized tasks are proposed IO tactical tasks.

Mission to Task Products

- **IO Mission Statement** — How IO will support the command's mission *(Who, What, Where, When, Why)*
- **IO Objectives** — What IO will do to affect the info environment *(Effect, Object of Effect [Target], Purpose of the Effect)*
  - 3-5 Objectives per Phase. **Caution:** Each IO Objective generates a Wargaming Worksheet.
- **Tasks to IO Elements** — What actions the elements will perform to execute the info op *(Task, Purpose)*
- **Tasks to Units** — Task, Purpose
- **IO Concept of Support** — How the info operation will be conducted *(Cdr's Intent for IO, Info Superiority for the Operation, General Plan for IO, Priority of Support, Restrictions on the Employment of IO)*

Offensive IO Effects

EFFECTS	DESCRIPTIVE EXPLANATION
DESTROY	Physically render adversary information useless or INFOSYS ineffective unless reconstituted.
DISRUPT	Break or interrupt the flow of information between selected C2 nodes.
DEGRADE	Reduce the effectiveness or efficiency of adversary command and control systems, and information collection efforts or means.
DENY	Withhold information about Army force capabilities and intentions that adversaries need for effective and timely decision making.
DECEIVE	Mislead adversary decision makers by manipulating their understanding of reality.
EXPLOIT	Gain access to adversary command and control systems to collect information or to plant false or misleading information.
INFLUENCE	Cause adversaries or others to behave in a manner favorable to Army forces.

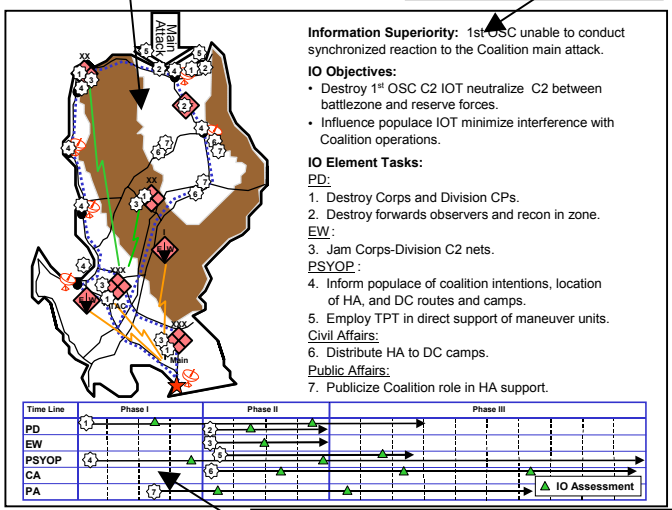
(FM 3-13)

Example Course of Action Sketch

(Deliberate Attack Mission)

Map of AO with locations of IO tasks

IO concept of support: objectives and tasks (for this mission)



Timeline (by phase) of IO task execution

U.S. Army, 1st Information Operations Command (Land) product updated by EWA-IIT (Garry Beavers)