



Integrating Information Operations with F3EAD Targeting

A Guide for U.S. Forces · February 2011

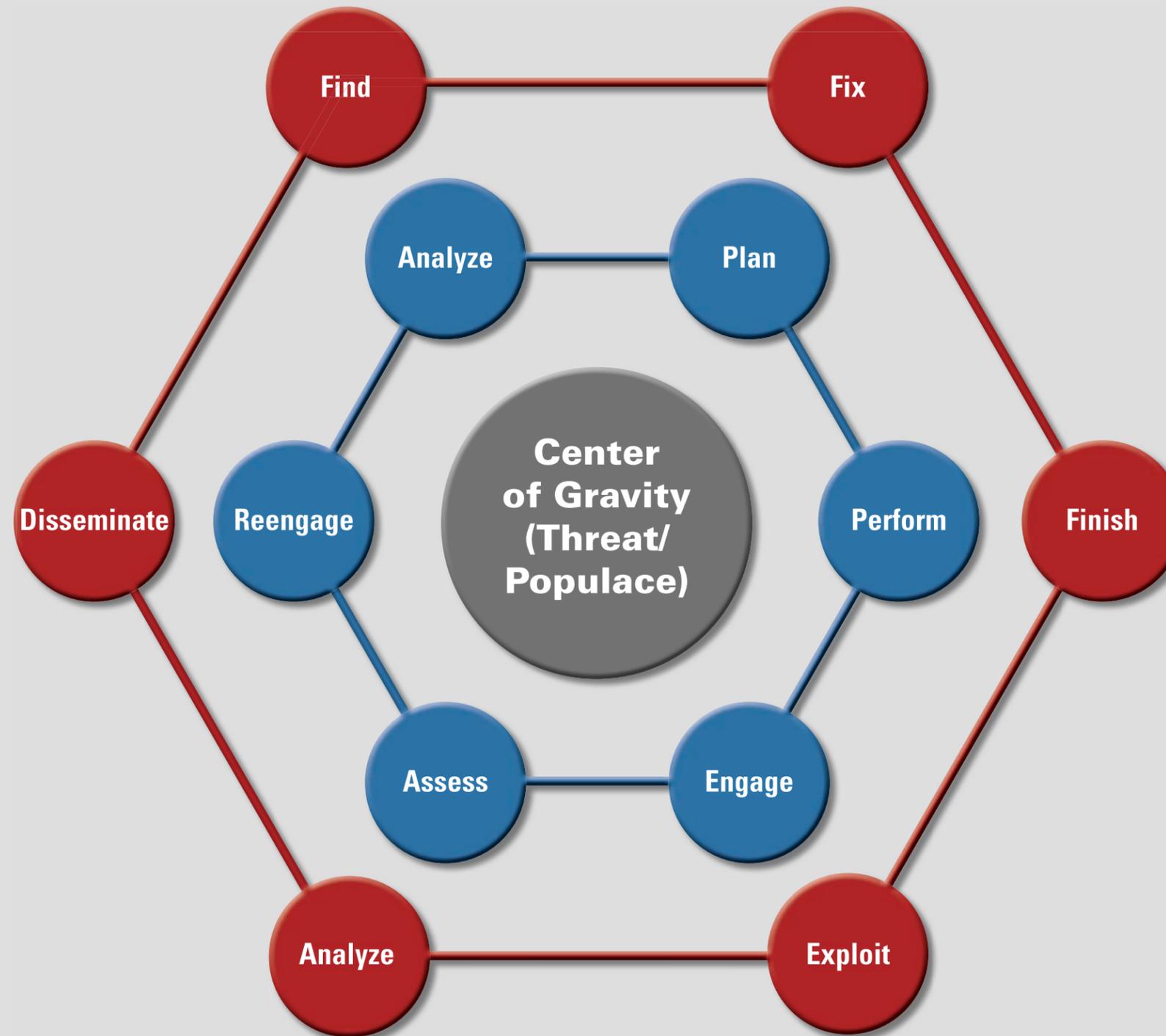
UNCLASSIFIED

Information Operations Integration Process with F3EAD

Information Operations (IO) are an integral part of the Find, Fix, Finish, Exploit, Analyze, and Disseminate (F3EAD) targeting process. When fused with other enablers, IO contribute to shaping the operational environment in the following ways:

- Influence both friendly and threat centers of gravity
- Identify or exploit threat critical vulnerabilities
- Deny or disrupt threat critical requirements

Effectively planned and holistically executed, IO result in gaining and maintaining informational superiority. This fusion allows Commanders to enhance the effects of all elements of combat power. Incorporating the core, supporting, and related capabilities offensively and defensively allows the desired effects to be achieved as an economy of force.



IO Integration

IO Integration is a continuous process that assists the planner in not only thinking about lethal targeting but also on how to incorporate IO to shape and exploit the battlefield.

- | | |
|----------|-------------|
| Analyze | Find |
| Plan | Fix |
| Perform | Finish |
| Engage | Exploit |
| Assess | Analyze |
| Reengage | Disseminate |

The **APPEAR** planning process is designed to run parallel to the **F3EAD** targeting process, allowing for economy of force during planning. This guide outlines and incorporates how APPEAR can be used with the F3EAD process.

Find/Analyze

Find

Define the network, find key personalities, and build patterns of life.

Analyze

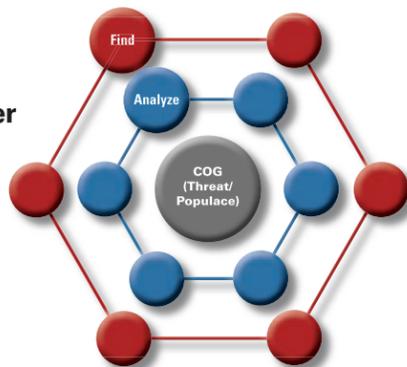
Define the network, atmospherics, and target audience (Threat, populace, or both). Adapt the IO activities to the specific network or targets.

Utilize Intelligence Fusion Throughout the Process

- **Standard ("INTs"):** Human, signals, imagery, measurement and signature, and open source intelligence
- **Non-Standard:** Law enforcement professionals, provincial reconstruction teams, civil affairs, human terrain teams, and agricultural development teams
- **Previous Exploitation:** Targets, patrols, key leader engagements (KLEs), and significant activities (SIGACTs)

Incorporate Cultural Advisor and IO Planner

- Refine IO intelligence preparation of the environment (IPE) and information overlay
- Initiate civil reconnaissance



Fix/Plan

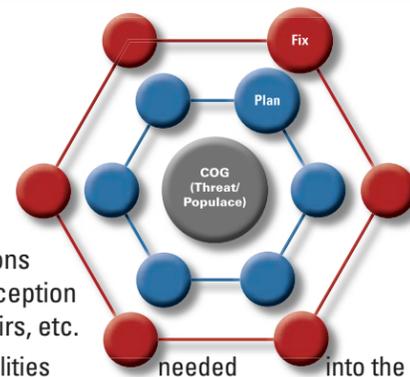
Fix

Fix the target to a location.

Plan

Plan IO objectives and tasks to the current target. Identify IO capabilities available to support operations: electronic warfare (EW), computer network operations (CNO), psychological operations (PSYOP), operations security (OPSEC), military deception (MILDEC), combat camera, public affairs, civil affairs, etc.

- Identify desired effects and incorporate IO capabilities needed into the plan
- Identify both populace's and threat's critical requirements/vulnerabilities
- Exploit target's (threat's) placement within the insurgency
- Neutralize target's placement within the community
- Plan for information/media release and outlets for immediate action
 - Identify most efficient delivery vehicle for information and exploitation efforts (i.e., local radio, radio in a box, KLEs, handouts, and/or face-to-face with the populace)
- Develop mitigation plan (plan for contingencies, personnel to contact, and actions to take)
- Plan KLE talking points and reengagement forces
- Identify IO assets available to achieve effects
 - PSYOP products available; prepare early for additional products if required
 - CNO opportunities that will support operations and exploitation
 - EW assets available to support desired effects



Finish/Perform

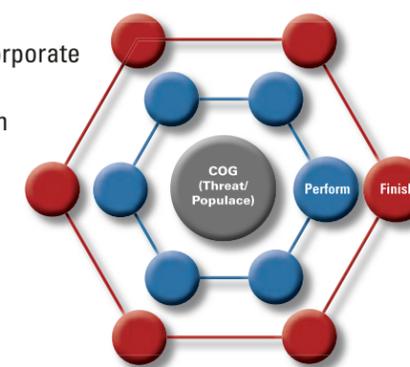
Finish

Carry out actions on the objective.

Perform

Execute IO tasks that support the objectives in order to shape operations. Maintain a flexible plan, and be prepared to incorporate consequence management.

- Information heard first is usually taken as fact
- Identify/ mitigate the threat's capabilities on target
 - Overpower, disrupt, or deny the threat's messaging capabilities
- Identify and emplace feedback mechanisms
- Take pictures before, during, and after in order to mitigate insurgent propaganda
- Incorporate local media if situation dictates
- Maintain flexible plan, and be prepared to incorporate mitigation efforts
 - Commander's Emergency Response Program (CERP) payments
 - Talking points
 - Photograph/video and press releases



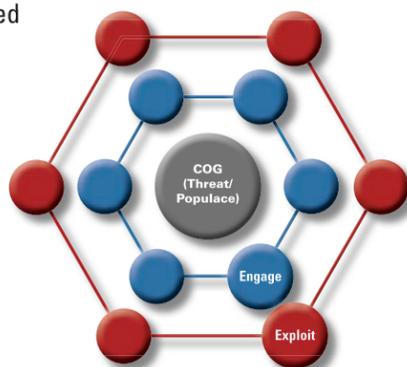
Exploit/Engage

Exploit

Apply tactical site exploitation (TSE) and tactical questioning (TQ).

Engage

- Know target audience threat/populace and adjust accordingly
- Conduct KLEs to get the message out first
 - Explain why you are there
 - Engage populace, key leaders, and neighbors in order to spread the correct information
 - Interview locals in order to exploit success through media efforts
- Utilize host nation forces, tactical PSYOP teams, combat camera, public affairs office (PAO), civil affairs, etc.—anything that will assist in achieving objectives and tasks
- Provide additional feedback mechanisms as needed
 - Acquire phones for key leaders
 - Get names and phone numbers
 - Provide hotline number
- Use onsite collection and be prepared to adjust efforts
- Exploit IO opportunities in order to reduce the threat's freedom of action/propaganda



Analyze/Assess

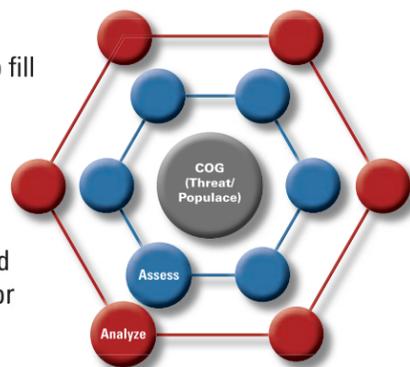
Analyze

Extract pertinent Intel from TSE and TQ in order to fill intelligence gaps and use for future targets.

Assess

Assess feedback mechanisms, atmospherics, Intel collection, and information from KLEs, TSE, and TQ to feed or adjust future messages and engagements. These will serve as assessments for future decision making.

- Be prepared to adjust reengagement plan
- Exploit feedback mechanisms
- Initiate media releases
- Assess whether planned assets worked for immediate measures of effectiveness
 - *How did the threat and populace respond to our actions?*
- Evaluate IO vehicle/message effectiveness and determine what IO activities might need to be adjusted
 - *What feedback mechanisms will work better next time?*
 - *What can be done better next time?*



Disseminate/Reengage

Disseminate

Feed the Intel and operational cycle.

Reengage

Adjust your IO tasks with Intel gained from the assessment, and reengage key leaders and those identified in the assessment. This is the most important step: it demonstrates action and disrupts the threat's decision cycle.

- Feed operational cycle with assessment
 - Feed both non-lethal and lethal targeting
 - Adjust collection and feedback assets as needed
 - Identify future engagements
- Detailed documentation of engagements and efforts will prevent the next unit from starting over and will sustain momentum
- Use most effective asset for reengagement
 - Reserve force
 - Higher command
 - Civil affairs
 - Agricultural development team
 - Human terrain team
 - Provincial reconstruction team
 - Tactical PSYOP team
 - Focused targeting force
- Be prepared to adjust IO objectives and tasks from all assessments

