Enduring Network Operational Assessment Framework

Session 6

Track 1: “Enabling the Joint, Coalition Counter-Insurgency Campaign”

Hugo Badillo
CENTCOM Programs & Architectures Division (CCJ6-P)
Purpose

**Synopsis:** This session will demonstrate that an effective enduring framework does not exist to synchronize and coordinate activities of all relevant commands and organizations to assess and mitigate the risk associated with networks deployed in the Afghanistan Combined Joint Operations Area (CJOA).

**Key Outcomes:** This session will appraise Services, COCOMs and Agencies of the importance of an enduring network operational assessment framework to improve IA/CND posture of existing networks.
Outline

★ Background
★ CX-I OA Framework as Baseline
★ Establishing an Enduring OA Framework
★ Summary

CX-I: CENTRIXS ISAF
CENTRIXS: Combined Enterprise Regional Information Exchange System
ISAF: International Security Assistance Force
OA: Operational Assessment
Background: Afghanistan Mission Network (AMN)

AMN is:
- NATO ISAF-Secret core
- National extensions
- The coalition warfighting network in Afghanistan

Nations connect by:
- Connecting National Systems
- Paying for NATO Systems

**CENTRIX ISAF (CX-I):**
US Extension to the AMN
First Afghanistan Mission Network (AMN) assessment was conducted by USSTRATCOM and USCYBERCOM in June/July 2010

- Focused on Global/Strategic Risk
- Report concluded the need for corrective actions and a Command Cyber Readiness Inspection (CCRI) in 2011

The CCRI was later changed to be the Operational Assessment (OA) to account for the interests and concerns of the three Commanders at the global/national, regional, and combined joint operations area (CJOA) level.
2011 CX-I OA Framework as Baseline (1 of 9)

★ Goals

• Identify, assess, and fix CX-I vulnerabilities
• Provide recommendations
• Establish baseline for an enduring CX-I OA framework

★ Risk Assessed for 3 Commanders

USFOR-A/COMISAF
USCENTCOM
USCYBERCOM

★ Assessed Risk to:

1. US Interests
2. US Networks
3. (Cyber) Key Terrain
4. Operational Framework

Session: 6, Enduring Network Operational Assessment Framework
Cyber Key Terrain is defined as physical or virtual elements in the network of such importance that they must be secured and defended to ensure mission success and the seizure or exploitation of which affords a marked advantage to the adversary.
17 Operational Assessment Areas (OAAs)

Some example OAAs are:

- C2 Applications
- Information Sharing
- Cross Domain Solutions
- Network Operations Framework/Tenets
- Sensors and Firewalls
- Network Interface Points
3 Dimensions of Risk Assessment

3 Commanders
- USFOR-A/COMISAF
- USCENTCOM
- USCYBERCOM

Regional
Global

4 Risk Areas
1. US Interests
2. US Networks
3. Key Terrain
4. OPS Framework

17 Operational Assessment Areas
1. Cross Domain Solutions
2. Information Sharing
3. Command & Control Apps
4. Insider Threat
5. NetOps Framework/Tenets
6. Sensors and Firewalls
7. Network Interface Points

and others...
Methodology for OA Execution

- Task force approach
- Leverage past assessments
- Assess stakeholder contributions
- Fix as we go – do no harm
- Remote execution as much as possible
- DOD standards as baseline
2011 CX-I OA Framework as Baseline (6 of 9)

**Functional Structure for OA Preparation and Execution**

- **Executive Committee**
  - Provide guidance to Senior Panel
  - Validate assessment
  - Inform Joint Staff

- **Senior Panel**
  - Execution Management/Synchronization
  - Report preparation

- **Operational Cell**
  - Facilitate day-to-day operations
  - Enable teams ability to perform assessments
  - Support Senior Panel

- **Focus Area Teams**
  - **Focus Area Team 1**
  - **Focus Area Team 2**
  - **Focus Area Team 3**
  - **Focus Area Team n**
    - Perform technical evaluations
    - Identify and assess findings
    - Provide input to OA Report

**Coalition Network Stakeholders Represented**

- Subject Matter Experts
  - from different government organizations

---

Session: 6, Enduring Network Operational Assessment Framework

2011-08-25 // U.S. Central Command J-6
CX-I OA Risk Levels and Definitions

<table>
<thead>
<tr>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HIGH</td>
<td>Achieving Objectives is Questionable</td>
</tr>
<tr>
<td></td>
<td>Shortfalls in Resources for CCDR Critical Requirements</td>
</tr>
<tr>
<td>SIGNIFICANT</td>
<td>Achieving Objectives is Likely</td>
</tr>
<tr>
<td></td>
<td>Resources Available for most CCDR Requirements</td>
</tr>
<tr>
<td>MODERATE</td>
<td>Achieving Objectives is Very Likely</td>
</tr>
<tr>
<td></td>
<td>Full Capacity to Source CCDR Requirements</td>
</tr>
<tr>
<td>LOW</td>
<td>No Impact to Operations</td>
</tr>
</tbody>
</table>

Lessons Learned: Risk Levels and Definitions should be consistent with the Chairman’s Risk Assessment Methodology
## Risk to Regional Commander by OAA for Applicable Focus Area

### Operational Assessment Area (OAA) for Applicable Risk Focus Areas

<table>
<thead>
<tr>
<th>Operational Assessment Area (OAA)</th>
<th>US Interest</th>
<th>US Networks</th>
<th>Key Terrain</th>
<th>OPS Framework</th>
</tr>
</thead>
<tbody>
<tr>
<td>OAA #1</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>OAA #2</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>OAA #3</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>OAA #4</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>OAA #5</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

### Critical OAA for Regional Commander

- OAA #1
- OAA #2
- OAA #3
- OAA #4
- OAA #5

### Overall Risk

- **X**: Will contain a defined risk rating: **Low** | **Moderate** | **Significant** | **High**
- **Not Applicable**
## Consolidated Risk to Commanders by OAA

<table>
<thead>
<tr>
<th>Operational Assessment Area (OAA)</th>
<th>CJOA Commander</th>
<th>Regional Commander</th>
<th>Global Commander</th>
</tr>
</thead>
<tbody>
<tr>
<td>OAA #1</td>
<td>×*</td>
<td>×*</td>
<td>×*</td>
</tr>
<tr>
<td>OAA #2</td>
<td>×*</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>OAA #3</td>
<td>×</td>
<td>×*</td>
<td></td>
</tr>
<tr>
<td>OAA #4</td>
<td>×</td>
<td>×</td>
<td>×*</td>
</tr>
<tr>
<td>OAA #5</td>
<td></td>
<td></td>
<td>×</td>
</tr>
</tbody>
</table>

**Overall Risk per CDR**

<table>
<thead>
<tr>
<th>CDR Commander</th>
</tr>
</thead>
</table>

*Critical OAAs are weighted [n] times more than other OAAs*

- **X** Will contain a defined risk rating:
  - Low
  - Moderate
  - Significant
  - High

- **Not Applicable**
Establishing an Enduring OA Framework (1 of 2)

★ **OA Framework by Phase**

- ✔ Phase 1 – Preparation
- ✔ Phase 2 – Execution
- □ Phase 3 – Implementation of Recommendations
- □ Phase 4 – Implementation of Enduring Framework

★ **Phase 3 – Implementation of Recommendations**

- Develop integrated priority list for fixing those findings with the most impact to the risk rating
- Refine priorities based on resources available
- Gain Executive Committee approval
- Coordinate resources and provide oversight for task execution
Phase 4 – Implementation of an Enduring Framework

- Establish an enduring Senior Panel and Executive Committee that represents all stakeholders
- Integrate the process into the normal activities of the standing day to day network operations framework
CX-I OA establishes a baseline for an enduring framework that balances the operate/provide and defend missions of the three Commanders at the global, regional, and CJOA.

An enduring OA framework would allow for synchronization and coordination activities between all relevant commands and organizations to assess, improve, and maintain the IA/CND posture of coalition networks and enable the warfighters to perform their operational mission.
Hugo Badillo

hugo.badillo.ctr@centcom.mil

hugo.badillo.ctr@centcom.smil.mil