Cyber Command & Control (C2)

Session 3
“Enduring Cyberspace Operations Command and Control Framework”

Colonel John Burger
Chief, Cyber Security
USCENTCOM CCJ6-C
Agenda

★ Background: The New Operational Domain
★ Purpose: Establish C2 Construct that satisfies the UCP assigned missions of all Commands
★ Key Facts
★ Operational Context / Imperatives
★ Scope of Cyberspace
★ USCENTCOM Model of Choice
★ Questions
“Cyber security threats represent one of the most serious national security, public safety, and economic challenges we face as a nation.”

- 2010 National Security Strategy

“Blue Cyberspace should have a different model. We will not come up with a once size fits all model to solve this complex issue.”

- BG Brian J. Donahue, Fmr Dir J6

“Neither government nor private sector nor individual citizens can meet this challenge alone – we will expand the way we work together.”

- 2010 National Security Strategy
Cyber vs. Conventional War fighting Domains.

- Cyber domain is not limited geographical boundaries; time and tempo (milliseconds) are unlike any other domain.
- Cyber effects are not limited to a single entity and may involve state and non-state actors.
- Cyber targets requiring military effects are geographically defined within a GCC’s Area of Responsibility.
- GCC must be able to coordinate and fully integrate cyber effects with kinetic and non-kinetic effects within their battle space.
## Operational Context

<table>
<thead>
<tr>
<th>Joint Crisis Action Phases</th>
<th>Phase 0 Shape</th>
<th>Phase 1 Deter</th>
<th>Phase 2 Seize Initiative</th>
<th>Phase 3 Dominate</th>
<th>Phase 4 Stabilize</th>
<th>Phase 5 Enable CIV Auth</th>
</tr>
</thead>
<tbody>
<tr>
<td>GIG Mission Sets (GNEC)</td>
<td>Generating Force CCDOR</td>
<td>Expeditionary</td>
<td>Campaign</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Supported CDR</td>
<td>Multiple</td>
<td>GCC</td>
<td>C/CJTF</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NETOPS Framework (Tenets)</td>
<td>Theater Based Global Enterprise</td>
<td>Increase Decentralization TIG to RCC</td>
<td>Begin Decentralization of CJOA Network to CDR CJTF</td>
<td>Increase Decentralization of CJOA Network to CDR CJTF</td>
<td>Compete Decentralization of CJOA Network to CDR CJTF</td>
<td>Begin transition Back to Theater Based Global Enterprise</td>
</tr>
<tr>
<td>Allocation Network Resources</td>
<td>Functional Supporting Commander</td>
<td>C/CJTF</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network Main and Supporting Effort</td>
<td>ME: IT Services – SE: Network Enabled Capabilities</td>
<td>ME: Network Enabled Capabilities – SE: IT Services</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network Focus</td>
<td>“Plug and Play” access to IT Services</td>
<td>Integrated CJOA Network – capabilities based</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sustaining a Campaign</td>
<td>Phase 0 – TOA Rehearsal Do not execute Phases 1-2</td>
<td>Admin Deployment – RSOI – Employment – TOA Directly into Phase 3/4 or 5 – METT-C Dependent</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

CCDOR = COCOM CDR Daily Operational Requirements  ME = Main Effort  SE = Supporting Effort
Joint operational Cyber C2 framework must be:

- Tenets based and account for full spectrum of conflict – and all operational phases of each.
- Aligned to operational chain of command.
- Enable all UCP assigned missions.
- Account for all networks that contribute to RCC and CDR CJTF Cyberspace – Combined/Joint C4ISR.

*Operational Framework for Cyber Space must account for all operational imperatives*
Commander’s Direction: Operational Network must enable:

- NATO coalition,
- Counter-insurgency (COIN),
- Long term campaigns,
- Immediate execution (anywhere the fight is…or goes…)

We are already planning and establishing the next Phase O Mission Network
The New Network Norm

Requirement: Move the fight to the coalition network.

→ To move fight, need to identify and move key war fighting missions functions.

→ To move mission functions, must move the applications that enable them.

→ To move applications, must move the data that populates the applications.

→ To enable all must establish a coalition network – In Afghanistan, AMN is foundational network.

New Norm: Must establish a Coalition network framework that moves the fight to the Coalition Network.
Scope of Cyber Space in CENTCOM - Area of Responsibility

**Red:** Cyber Battle Space: Attack – Exploitation – CND Response Actions  
CYBERCOM -- *is equal to* -- CENTCOM

**Blue** Cyber Battle Space: Provide and Defend (-) Dimensions  
CYBERCOM -- *is less than* -- CENTCOM

<table>
<thead>
<tr>
<th>Blue Battle Space Networks</th>
<th>CYBERCOM</th>
<th>CENTCOM</th>
<th>CJOA-A</th>
</tr>
</thead>
<tbody>
<tr>
<td>NIPRNET / SIPRNET</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>INTEL Community (JWICS)</td>
<td>+</td>
<td></td>
<td>+</td>
</tr>
<tr>
<td>Coalition</td>
<td>+</td>
<td></td>
<td>+</td>
</tr>
<tr>
<td>Combined Joint TF specific</td>
<td></td>
<td></td>
<td>+</td>
</tr>
</tbody>
</table>

CENTCOM: 26 Total networks – 24 outside scope CYBERCOM  
CJOA-A: 26-30 Total network – 24-28 outside scope of CYBERCOM
Global Cyber Space Framework

COA 1: Execute global framework from CYBERCOM through Cyber Command Service Components

+ Enables most Phase 0 Activities.
- Does not account for full scope of Cyber.
- Does not account all UCP assigned missions.
- Does not enable CJTF.
- Does not enable a joint theater network.

COA 2: Execute global framework through Regional Combatant Commands

+ Enables CJTF.
+ Accounts for full scope of Cyber.
- Will not work in CONUS
- Does not enable Generating Force.

COA 3: Execute through a Hybrid framework - RCC and Service Components.

Both COA 1 and 2 are infeasible.
Fundamental Mission Planning: Determine which mission sets are best executed at each Echelon -- Who is best postured to support?
Cyber C2 Way Ahead

Proposal at the GCC Level

- **Air, Land, Sea, Space and now... Cyber:** Establish a Regional Cyber Component; synchronizing and integrating the actions of cyber forces across all the dimensions of the cyberspace domain throughout the JOAs and CENTCOM cyber areas of interest / activity

Why treat Cyber C2 any differently?

- It starts in the CJOA: Warfighting Commander must assess the battlespace.
- Determine what missions and authorities are appropriate at which echelon. Then decide the optimal resource allocation and corresponding supported/supporting relationship BY MISSION THREAD.
- Establish a C2 Construct that ensures Unified response / shared awareness
- Cover full spectrum of Cyber Operations – 4 Dimensions
  - Provide, Defend, Attack, and Exploit
- Look beyond NIPR & SIPR – full scope of red & blue Cyberspace