Collaboration, Interoperability, and Secure Systems

May 21, 2008

Foundation for Interoperability

- Human aspects of “networked” operations
- Education and training
  - Doctrine
  - Organization
  - Business Process alignment
- Systems design
  - Data required
  - Use of Data provided
  - Tactics, Techniques and Procedures
It is DoD policy to improve communications and mutual understanding within the Department of Defense, with other Federal Agencies, and between the United States and its allies through the standardization of military and associated terminology.

The Chairman of the Joint Chiefs of Staff shall develop, issue, and maintain [Joint Publication 1-02, DoD Dictionary of Military and Associated Terms]

DoD Directive 5025.12, Standardization of Military and Associated Terminology

Joint doctrine is authoritative guidance and will be followed except when, in the judgment of the commander, exceptional circumstances dictate otherwise.

Use of joint doctrine standardizes terminology, training, relationships, responsibilities, and processes among all US forces to free joint force commanders (JFCs) and their staffs to focus their efforts on solving the strategic, operational, and tactical problems confronting them.

Joint doctrine applies to the combatant commanders, subordinate unified commanders, JTF commanders, subordinate component commanders of these commands, as well as forces assigned or attached to these commands.

When the Armed Forces of the United States participate in multinational operations, US commanders should follow multinational doctrine and procedures that have been ratified by the United States.

CJCS Instruction 5120.02A, Joint Doctrine Development System
Foundations for Collaboration

• **Fundamental questions**
  – What are we “looking at” (what is the situation)?
  – OR
  – What are we going to do about the situation?

• **Shared Situational Awareness**
  – Shared information (Data with CONTEXT)
  – Shared business process understanding (semantic alignment)
  – Necessary but insufficient conditions
    • Network connectivity
    • Interface tools

Joint & Combined Ops

Multilateral Interoperability Programme
Today's Systems: Aggravating the Boundary Problem

User Interfaces

Software

System of Record A

Software Routines

System of Record B

Software Routines

Data Bases

DataBase

DataBase

The Battlefield

Today's Information Systems (GIG CRD’s “Islands of Interoperability”)

Lesson Learned from Operation Iraqi Freedom - 2007

Stove-pipe functionality continues to function within the technical battlefield functional areas

“Business Process” analysis is required.

We continue to relearn the lesson that technology absent an operational concept is not a solution.

Unit LNOs to the Corps are tasked to cut event data contained in CPOF and paste the information into CIDNE.

The “storyboard” (PowerPoint slides that use map backgrounds and the common terminology and graphics standardized and codified in doctrinal publications) has become the defacto tool-of-choice for backbriefs at all echelons.

Units often default to the use of MS Office rather than the Systems of Record.

COL Harry Greene, PM-BC, and COL Roger McDonald, TRADOC Capabilities Manager, BC, after trip to Iraq
Problem: Security

• The Balance:
  – Need to Share
  vs.
  – Need to Protect

• Opportunity
  – Use the power of Shared Semantics
    Coupled with
  – Strong security engineering
    To
  – Enable discrete, protected, policy-based information sharing

COSMOS – Transformational Effort

• Operational problem from MARFORCENT OIF experience: sneaker-net info sharing impeded operations and led to confusion
  – Apply draft NSA Multinational Information Sharing (MNIS) Protection Profile
  – Implement the Multilateral Interoperability Programme (MIP) Common Interface (MCI)
    • What do the data bits mean? ▸ C2/JC3IEDM
    • How do we share the bits? ▸ MCI Data Exchange Mechanism

• Protected private C2 information sharing in the multinational environment.
  – Leverages the structure of the MIP C2 data model (C2IEDM->JC3IEDM)
  – Decomposes Cross Domain Solution (CDS) boundary functionality into coalition boundary functions separate from the National boundary
  – Implements the MCI in accordance with Information Assurance engineering design standards (NSA ISSE supervised)
  – Addresses many of the MNIS gaps

• Bidirectional information sharing:
  – Agile information dissemination/access management based on role and operational context (e.g., an organization’s assigned task, status, location, command relationships, etc)
  – Strong inbound data checking and protection
Joint Consultation Command and Control
Information Exchange Data Model
(JC3IEDM)

• Description:
  – Scope: war ops, crisis response, humanitarian
  – Core C2, generally country, military service, application, functional
    service, technology, vendor neutral
  – Logical, generic

• Net-centric adoption/direction:
  – Open standard (NATO STANAG 5525)
  – US Army - Battle Command and M&S
    • MCS 6.4 has MIP
    • ABCS SWB 10-12 will have PASS <-> MIP interface
    • Future Combat System
  – US Marine Corps - Core Information Model
  – Global Force Management - All US assets (hardware, people,
    organizations and associations)
  – ATP-45 Multinational CBRNE
  – Modeling & Simulation - Simulation Interoperability Standards
    Organization (SISO), JFCOM Joint Training

COSMOS Conceptual Architecture
Layered Model

- COSMOS builds trust as you move up
- Static Type 1 Core
- COTS AES 256 VPN Layer
- IP and Port associated with Sharing Contracts
- Sharing Contracts Enforced through Multi-Layered Controls

US COSMOS Node
Strong IA controls for using MIP on a multi-partner network

Increase of information flow across both boundaries

Does not require US to be in the middle of all MNIS flows

---

This is my HQ pit after returning from a patrol in the city

The insurgents undoubtedly work our seams. They do it in a couple ways. First is the obvious - figure out what point our patrols turn around or don’t seem to have firm control and conduct or stage for attacks there. The extra time it takes us to deconflict cross-boundary for fires and maneuver buys the insurgents the extra minutes they need to egress.

Second, and more problematic, is the method of living in one AO and conducting attacks in another. The insurgents have a clear understanding of our battalion AOs. Cells that operate in one battalions AO will conduct the majority of their operations in the neighboring ones. That way the Bn looking for the local [expletive deleted] has more difficulty finding them. Whenever we question the locals "where is the takfiri or erhabi" we are told the guys that did the attacks are "not from around here" or "are outsiders". Nobody knows who they are. We find this hard to believe but it’s often true. This is often incorrectly interpreted by us as meaning foreign fighters.
HUMINT is 95% of the fight for us.

Because basically all information is classified SECRET the primary problem is info sharing between adjacent units. The EN does not conveniently confine their activities to a certain battalion’s battlespace, some bad guys even figure out our seams and use them to their advantage. We found this to be the case in the AO I just left. Fixing that problem is the concern of the higher unit. With the connectivity we have, the phones, chat, websites, emails, the tools are all there. It isn’t a matter of new gear its a matter of using what we have and developing sound TTPs. It's a leadership issue.

Intelligence Officer, 1st Battalion, 1st Marines, April 14, 2005, shortly after the battalion redeployed from Baghdad