AFCEA TECHNET LAND FORCES EAST

"Toward a Tactical Common Operating Picture"

LTC Paul T. Stanton

OVERALL CLASSIFICATION OF THIS BRIEF IS
UNCLASSIFIED/APPROVED FOR PUBLIC RELEASE

"Transforming Cyberspace While at War… Can't Afford Not To!"

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
AUG 2012		**00-00-2012 to 00-00-2012**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Transforming Cyberspace While at War...Can't Afford Not To!	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Army Cyber Command/2nd ARMY,Fort Belvoir,VA,22060**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
Presented at the AFCEA TECHNET LAND FORCES EAST Conference, Aug 14-16, 2012, Baltimore, MD

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**19**	

Agenda

- Why a new COP?
- Unified Land/Cyber operations
- Distributed analytics and COP
- Consistency and commonality
- Considerations for tactical edge
- Questions and discussion

Why *Another* COP?

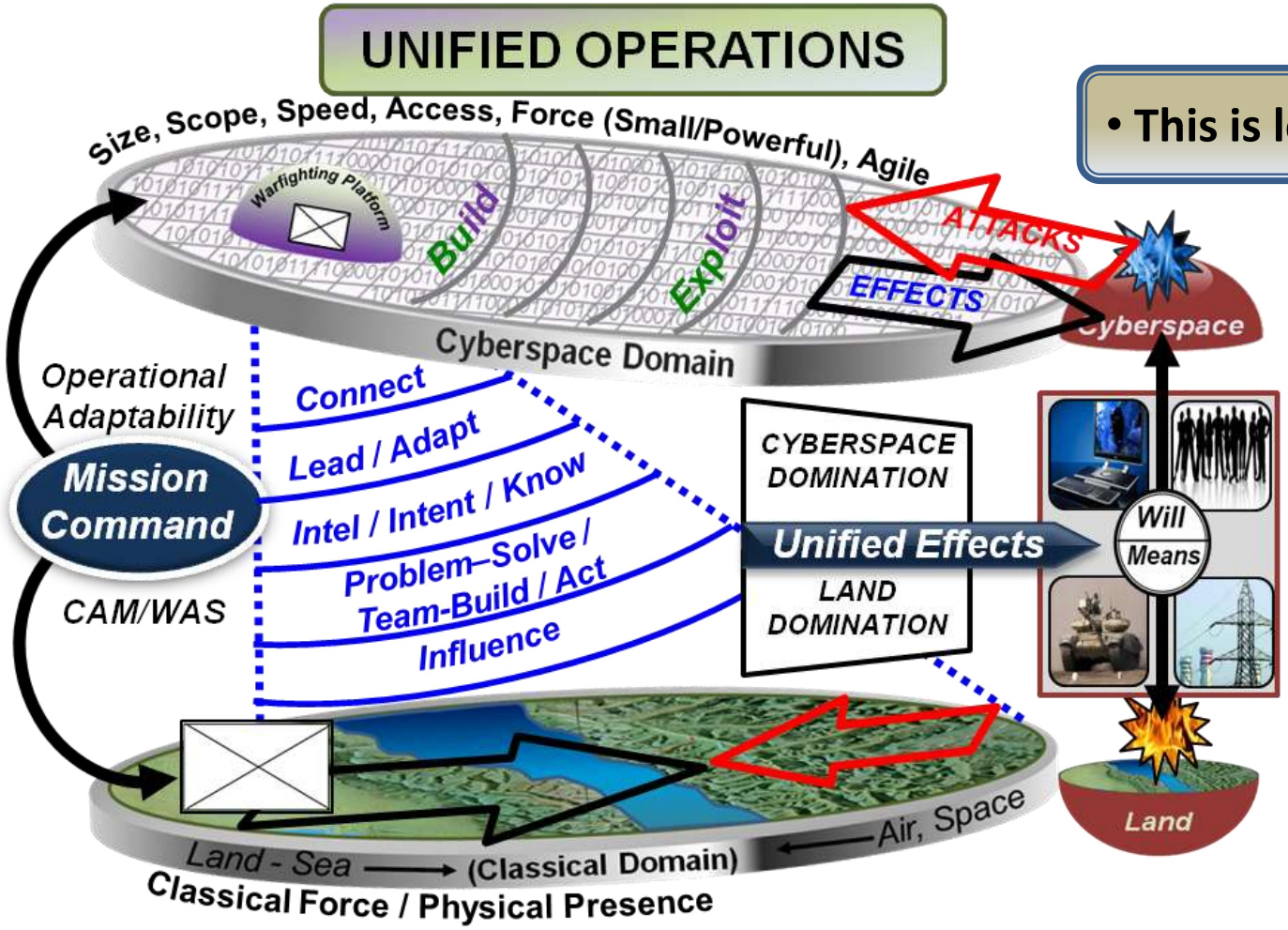
- Operations in the Unified Land/Cyber domain require effective Mission Command

- Mission Command is enabled by analyzing and visualizing the operational environment to provide **situational understanding** that supports **leader decision-making** in real-time

- Existing approaches lack integration

> "Mission command supports our drive toward operational adaptability by requiring a **thorough understanding of the operational environment**…"
>
> - GEN Dempsey

Land/Cyber



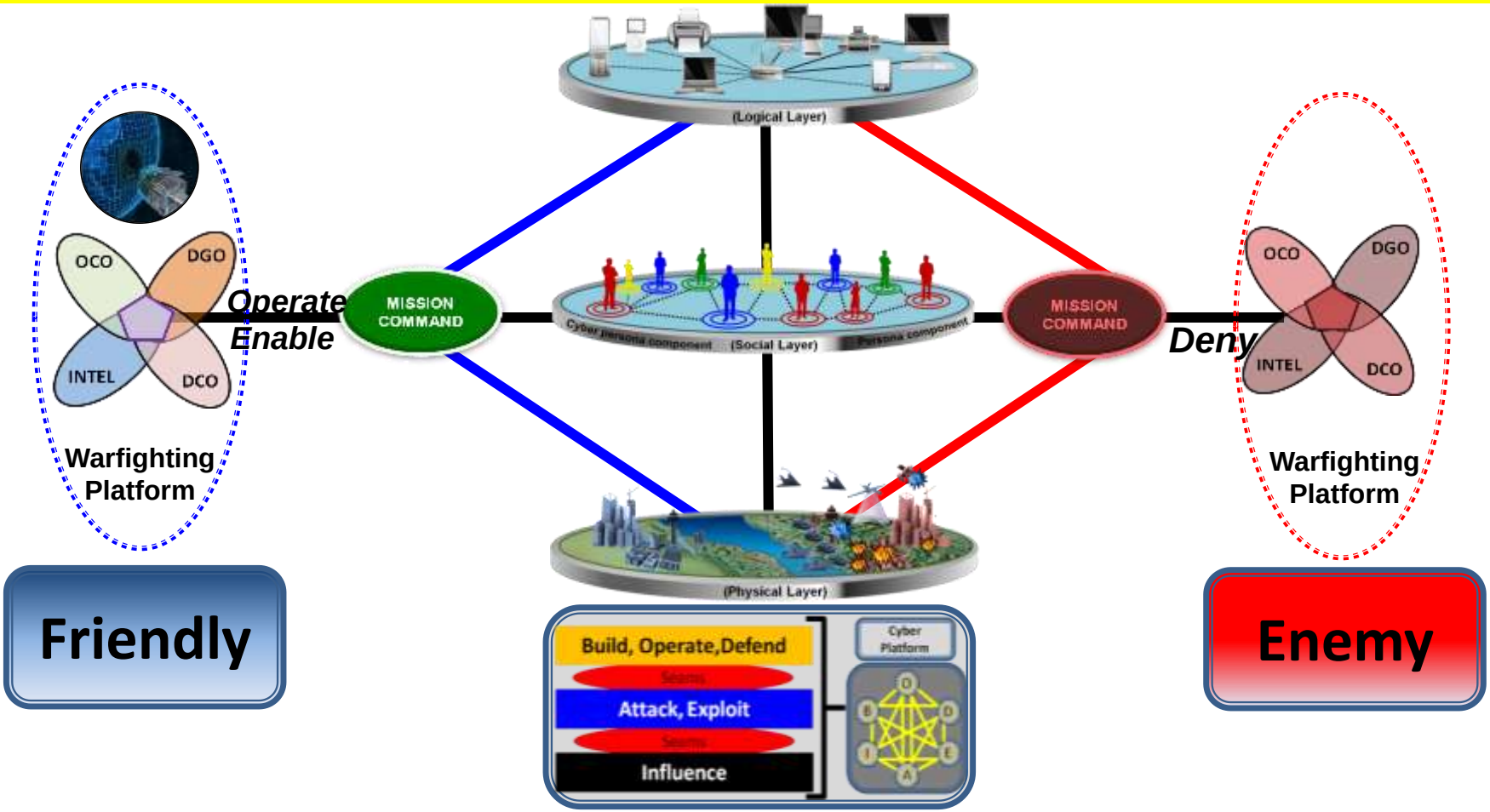
- This is leader's business

Prevent
Shape
WIN

*Mission Command applies **unified force** (Land and Cyber) to establish optimal combination of effects to achieve objectives*

"Second to None!"

Warfighting Platform



- Treat the network as a Weapon System
- Embrace cyberspace as a contested domain
- Strong 2-3-6 integration

"Second to None!"

Example "Terrain"

Political
Military
Economic
Social
Information
Infrastructure
Physical Environment
Time

Adversary
- Malware
- Malware developers
- Malware protocols
- Exploits
- Exploit developers
- Origin networks
- Callback domains
- Botnets
- Compromised credentials
- ……

Common
- Hosts
- Network Infrastructure
- Operating system
- Applications
- Architecture
- ……

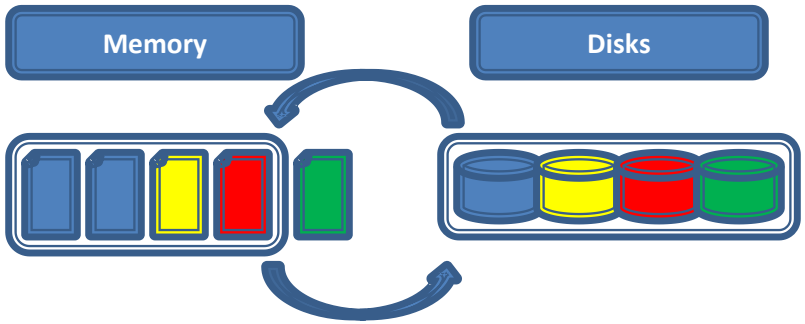
Friendly
- Host-based protection
- Sensors
- Offensive capabilities
- Incident responders
- Users
- Perimeter protection
- Points of presence
- Operators
- Passwords, CAC, PKI
- ……

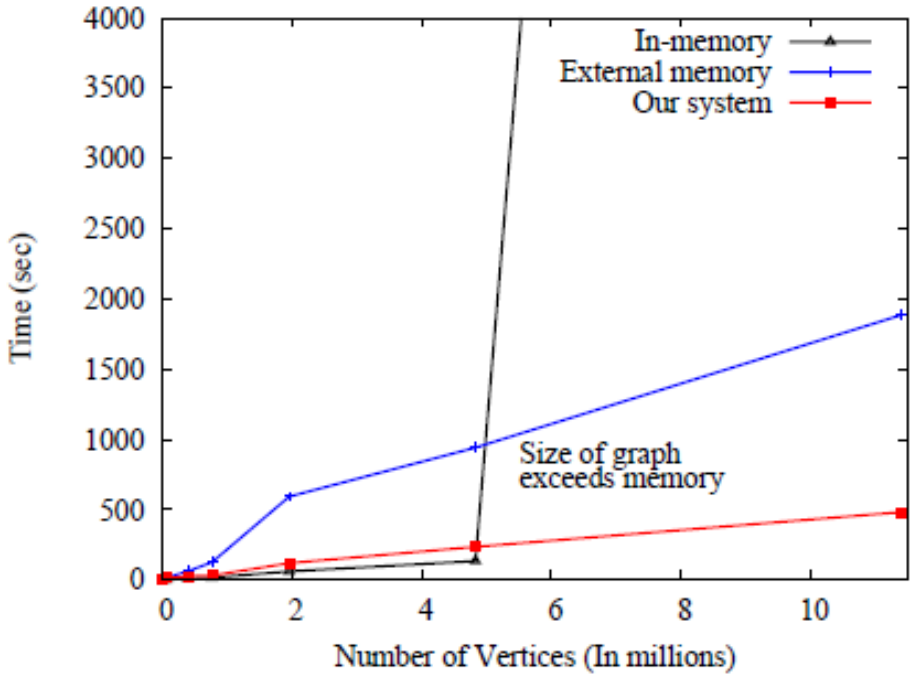
Big data, complexity of interaction / relationships

Big Data Solution

- "Seeing" the battlefield requires cloud Big Data analytics
  - Terrain is data
  - Terabytes daily, petabytes of historic data
  - Distributed data collection and computation

- Cloud vs Database
  - Databases optimize storage efficiency
  - Cloud uses "cheap" hardware to process in parallel

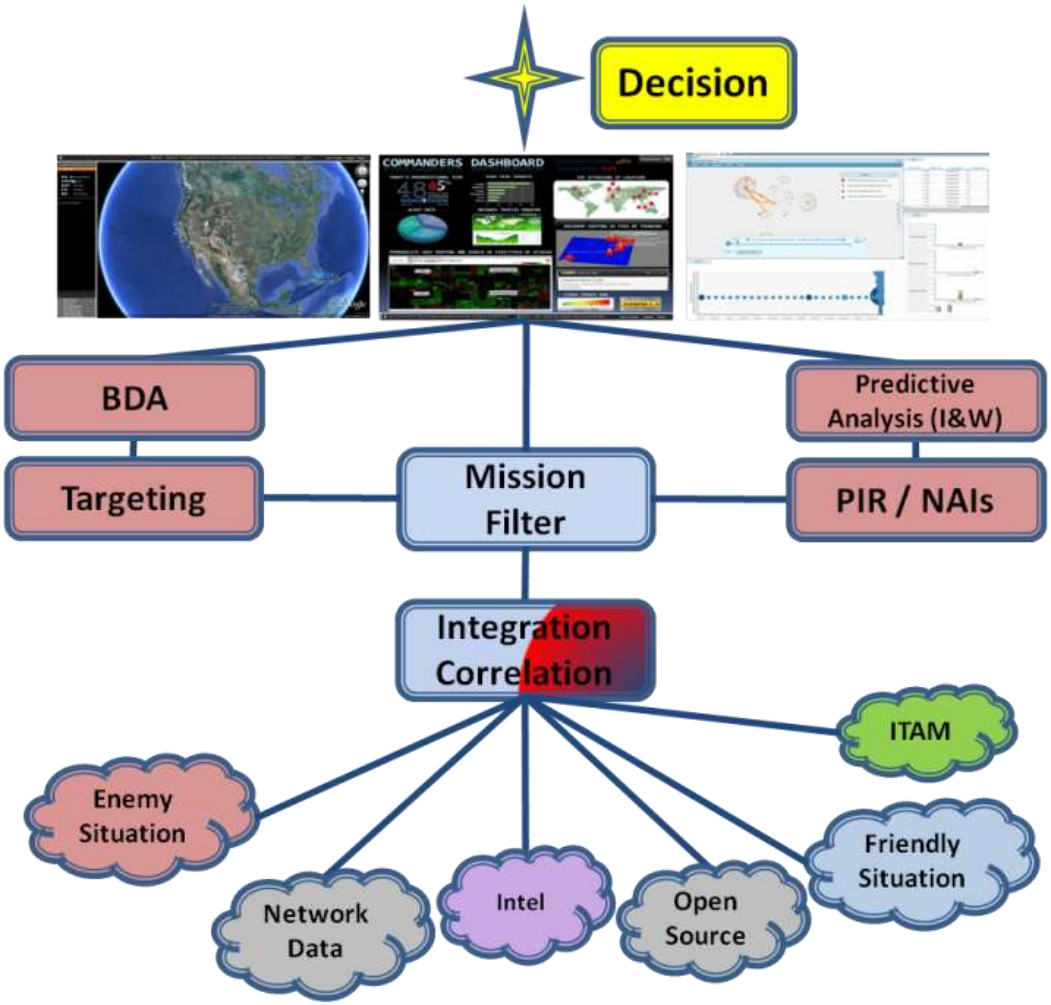




Enabling Mission Command

Visualization that supports leader decisions

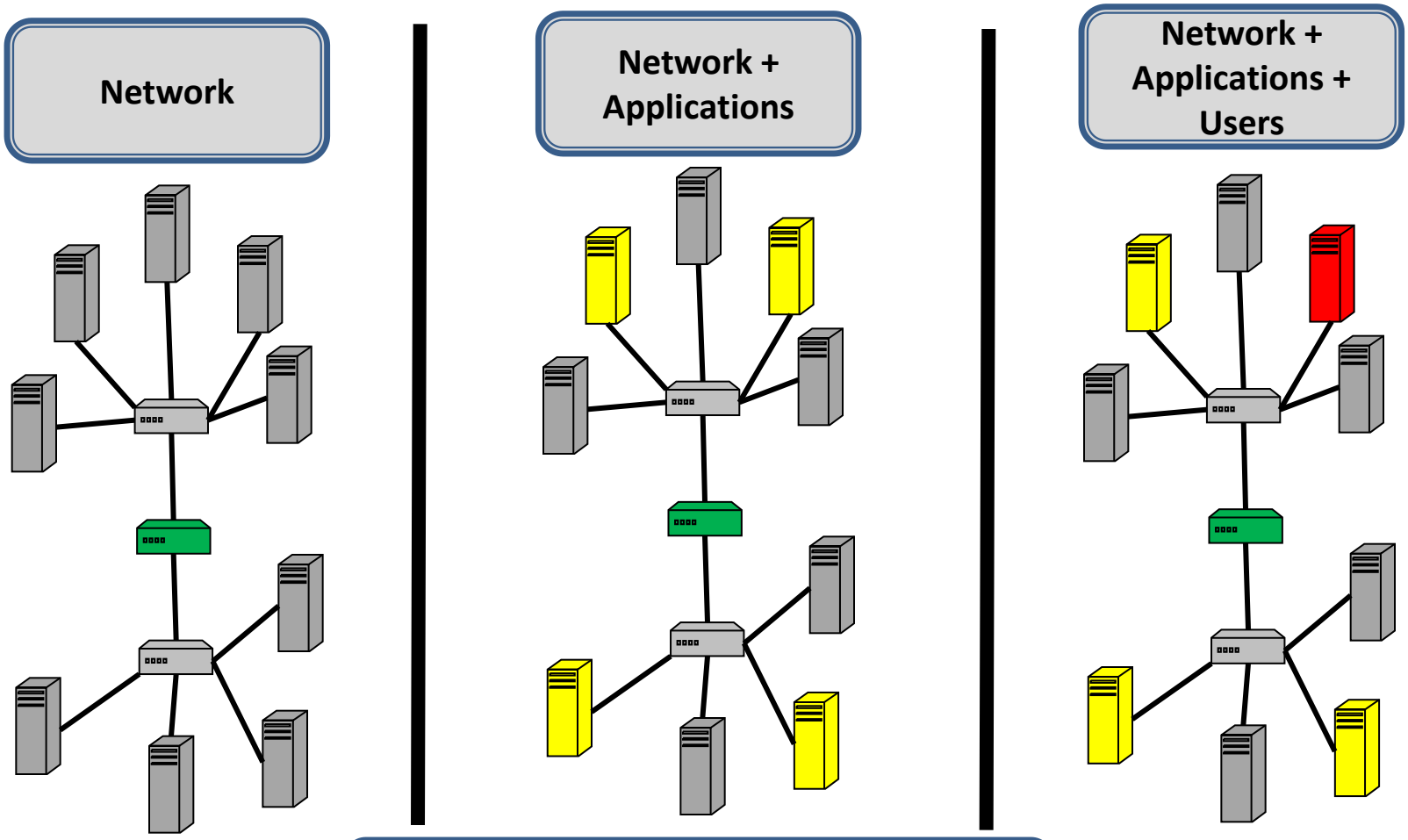
- **This is leader's business**



"Mission command emphasizes the importance of context …"
- GEN Dempsey

Key Terrain

- Mission focused overlays

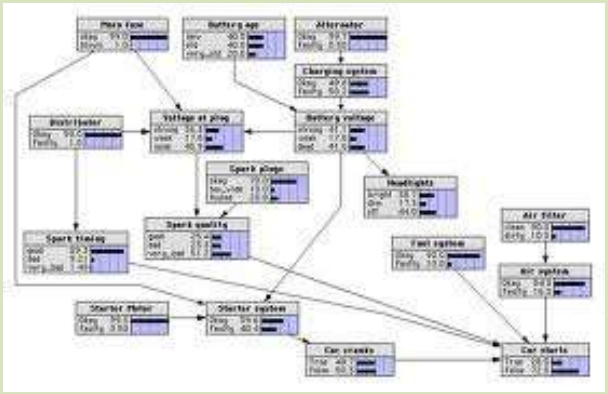


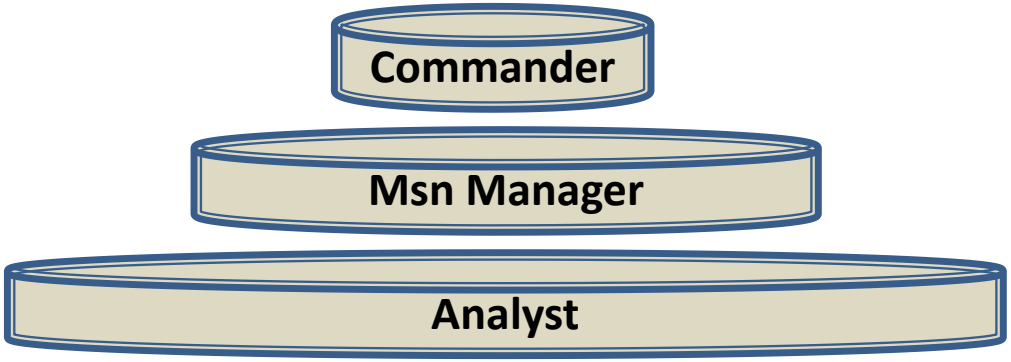
Anatomy of Visualization

Commander's Critical Information Requirements

"It really is the commander's *coup d'ceil*, his ability to see things simply, … that is the essence of good generalship." -- Clausewitz

Indicators & warnings → **Analysis** → **Queries** → **Bayes Net** → **Meter**



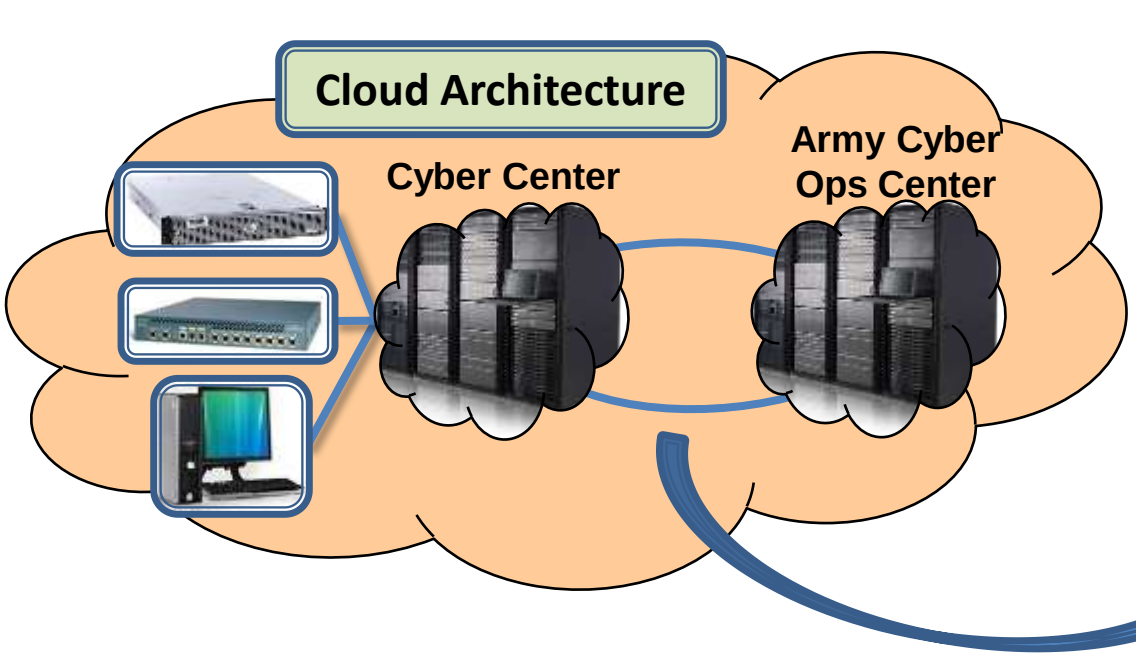


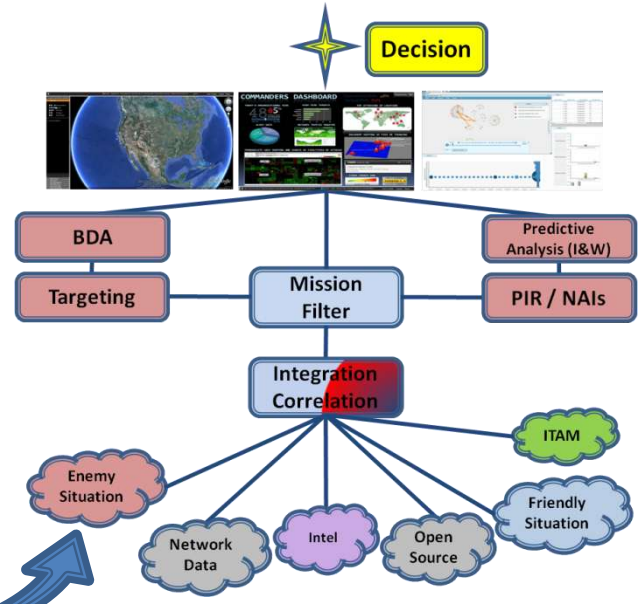
Considerations

- Data fidelity
- Scope of responsibility
- Data quantity / access

System Architecture

- Enforce compliance with basic standards
- Support IT reform



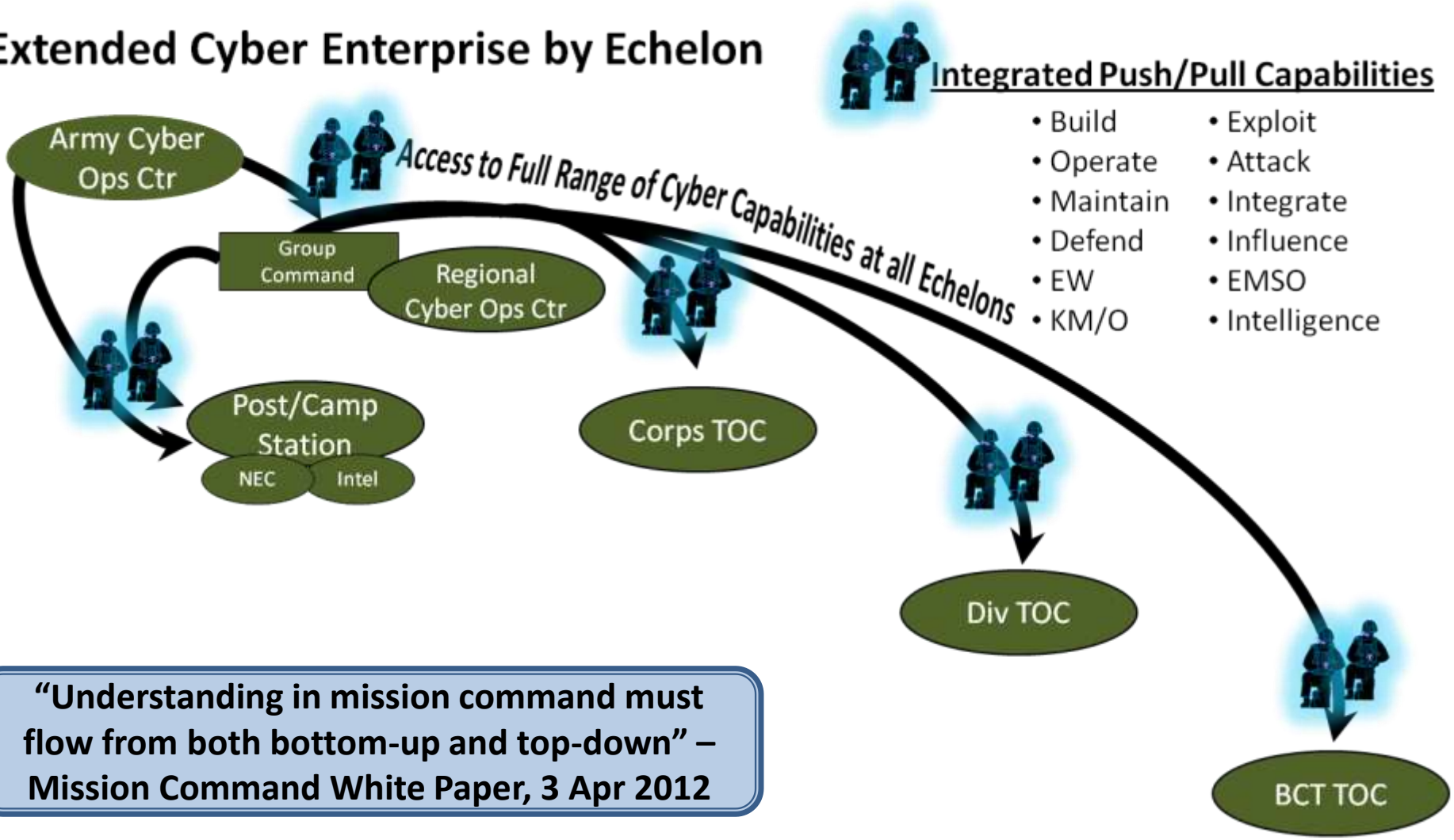


***Common* architecture, *common* data,**
***common* suite of pluggable visualization tools**

"Second to None!"

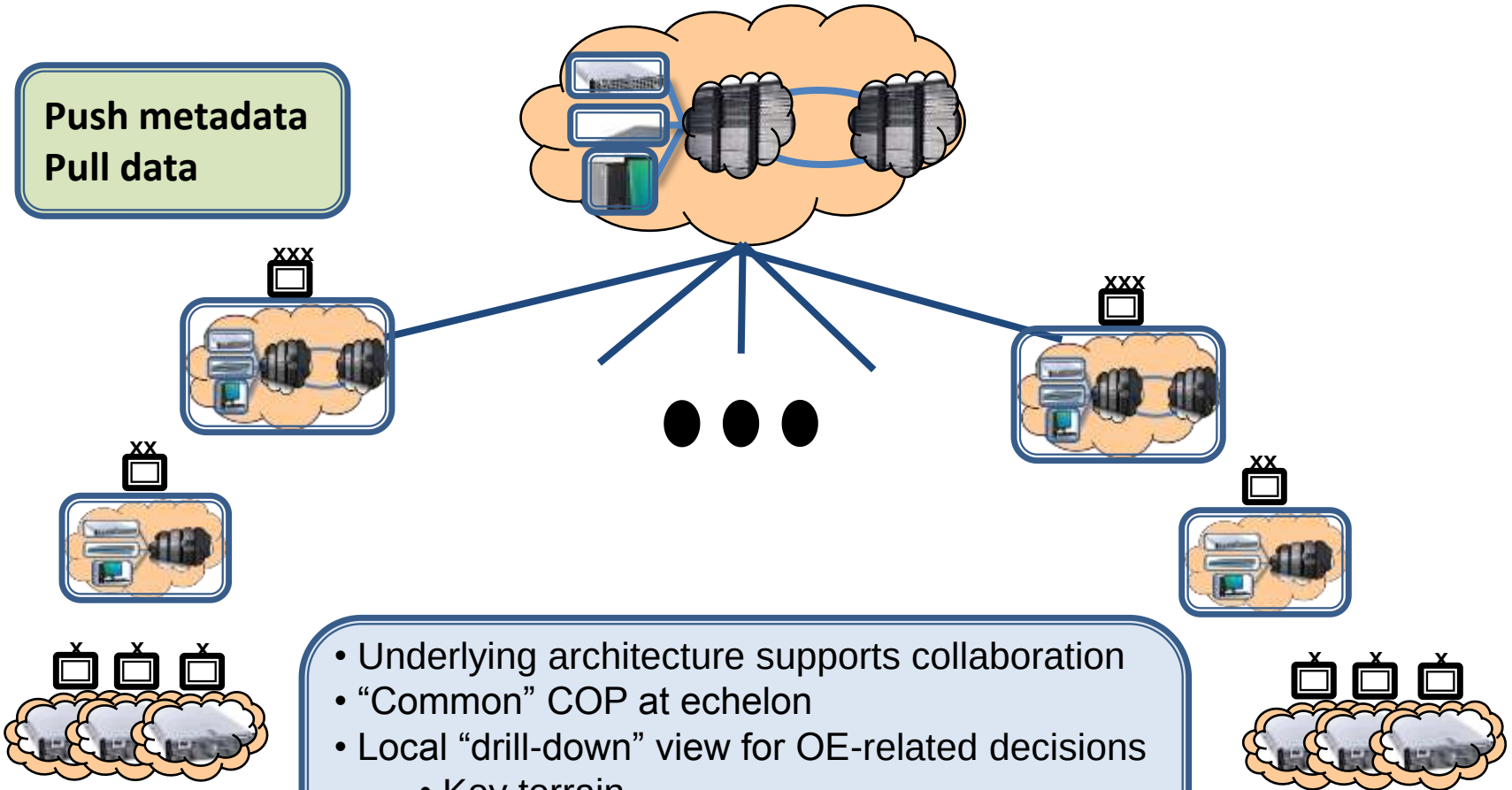
Reaching the Edge

Extended Cyber Enterprise by Echelon



"Understanding in mission command must flow from both bottom-up and top-down" – Mission Command White Paper, 3 Apr 2012

Consistency and Commonality



- Underlying architecture supports collaboration
- "Common" COP at echelon
- Local "drill-down" view for OE-related decisions
  - Key terrain
  - PIR / NAIs
  - Localized predictive algorithms
- Data / visualization subject to authorization

Tactical Considerations

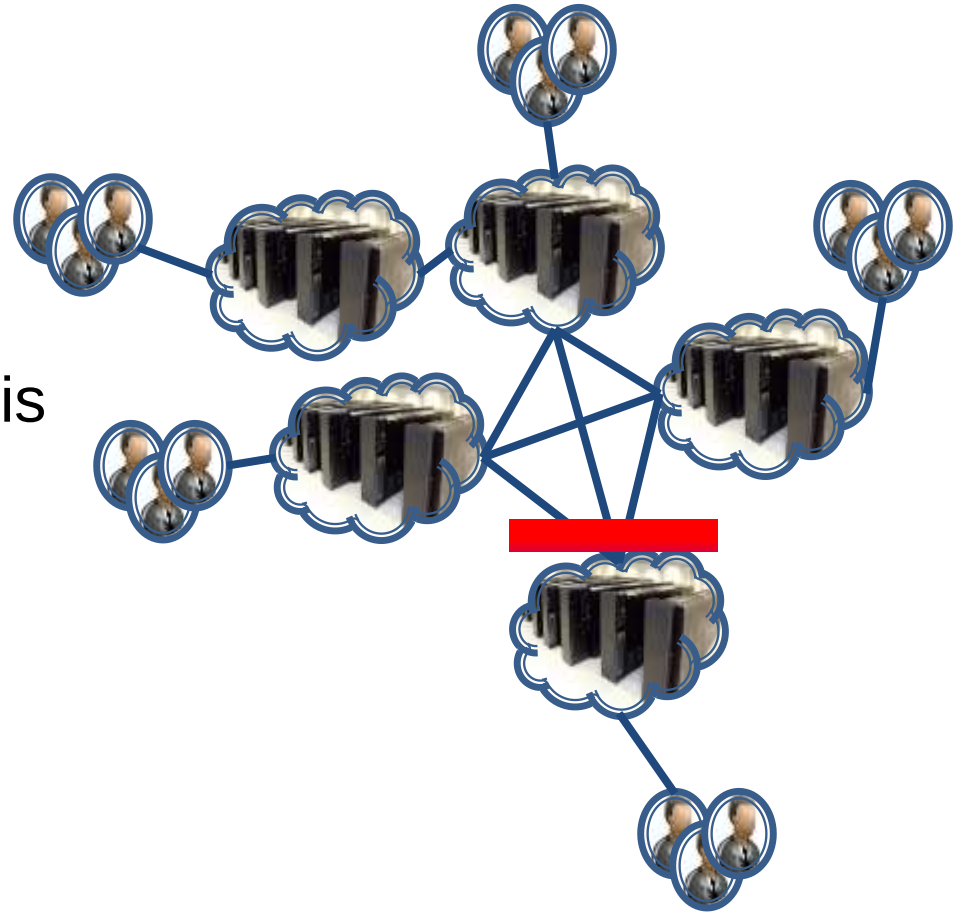
- Transition networks to a warfighting platform
- Workforce
  - Soldier and leader education and training
  - Manpower

  • Conduct training and leader development
  • Make people the centerpiece

- Physical limitations: bandwidth, power, connectivity
- Authorities
- Security
- Cost

Distributed Systems

- CAP Theorem
  - Consistency
  - Availability
  - Partition Tolerance
- Cloud storage – solution is mission dependent
  - Facebook
  - Military mission

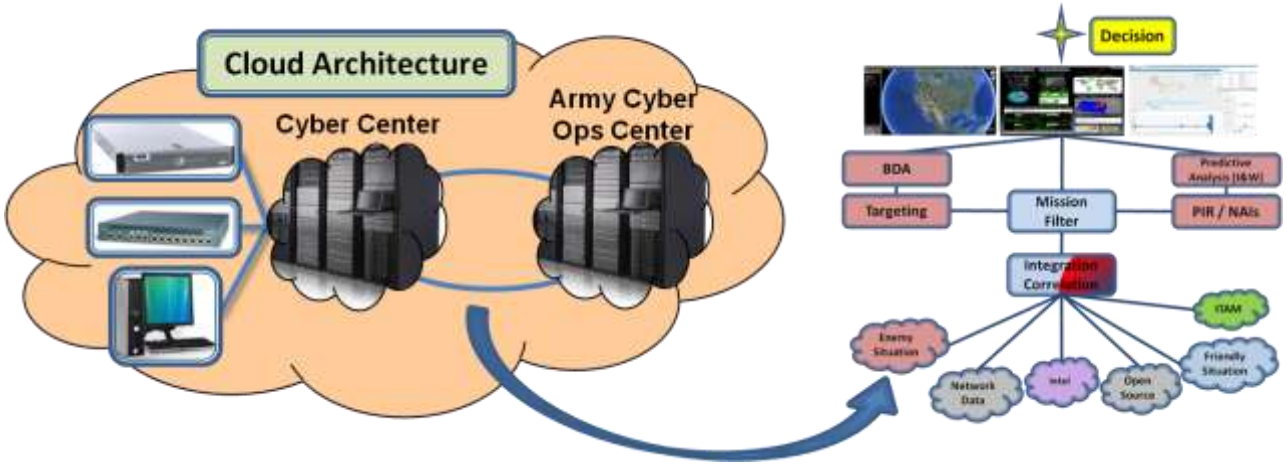


System design must account for network partitions that will be common in tactical environments

Way Ahead

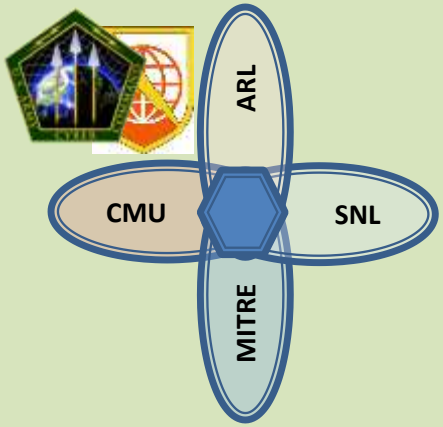
Goal

Analyze and visualize the operational environment to provide situational understanding that supports leader decision making in real-time



Army Cyber and NETCOM Initiative:

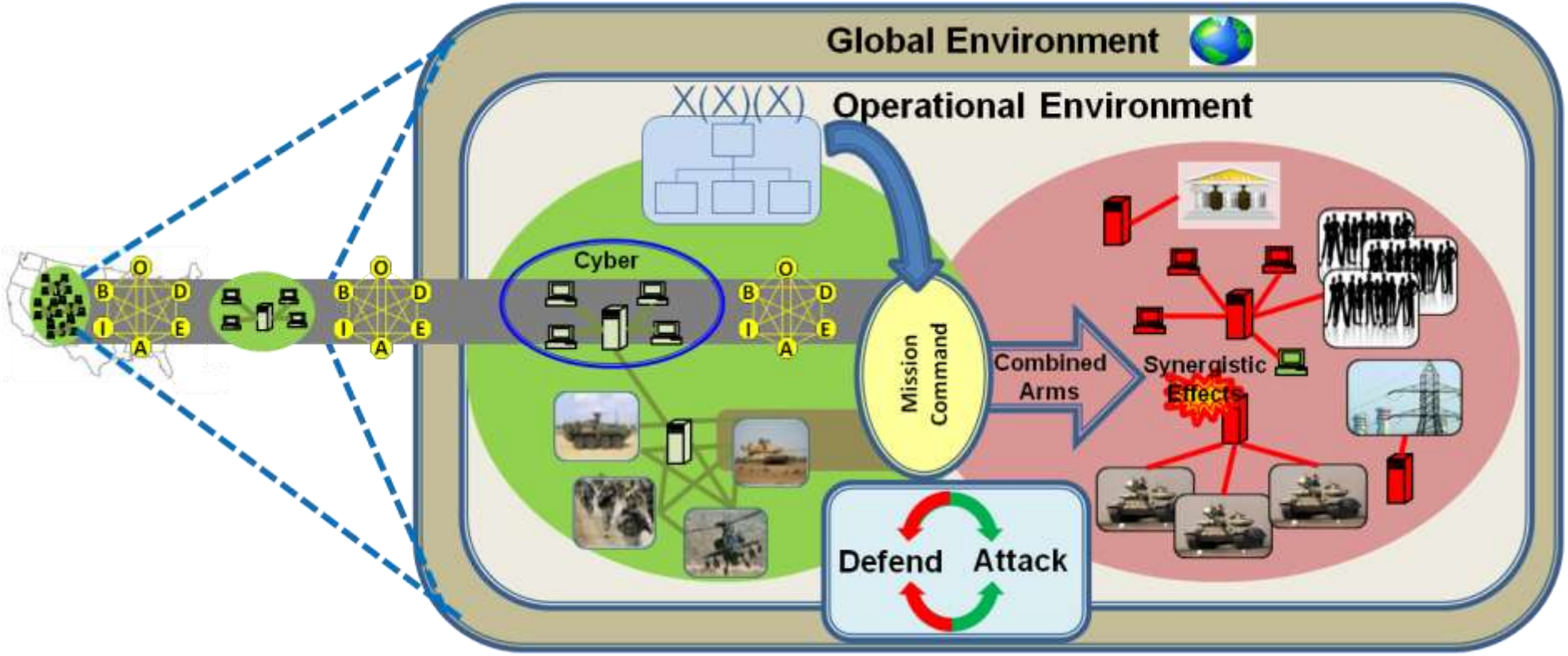
- 2 node proof of concept
- Support to an Army Command
- Participation from:
  - Carnegie Mellon University / Software Engineering Institute
  - MITRE
  - Sandia National Laboratories
  - Army Research Laboratories



"Second to None!"

Land/Cyber Synergy

Decision support to Prevent, Shape, **Win**



Summary

- A tactical COP must account for unified Land/Cyber operations
- Cloud-enabled commonality stems from data, architecture, and pluggable visualization tools
- Tactical deployment must account for hard distributed system problems

QUESTIONS AND DISCUSSION