

Adapting C2 for the 21st Century

presented to

12th International Command and Control
Research and Technology Symposium
Newport, RI
June 2007

Dr. Linton Wells II
National Defense University

Bottom Line - Up Front

- NCO is delivering today
- Challenges Remain
- Must Adapt C2 Concepts and Approaches
- Must Achieve Capability for Assured Information Sharing and Collaboration Beyond the DoD

Transforming National Defense



National Security Strategy

Transform America's national security institutions to meet the challenges and opportunities of the twenty-first century.



National Defense Strategy

We will conduct network-centric operations with compatible information and communications systems, usable data, and flexible operational constructs.

Beyond battlefield applications, a network-centric force can increase efficiency and effectiveness across defense operations, intelligence functions, and business processes...

Transforming to a network-centric force requires fundamental changes in process, policy, and culture.



National Military Strategy

...creation of a collaborative information environment that facilitates information sharing, effective synergistic planning, and execution of simultaneous, overlapping operations... on demand to defense policymakers, warfighters and support personnel.

Transforming National Defense



National Security Strategy

Transform America's national security institutions to meet the challenges and opportunities of the twenty-first century.

21st Century challenges



National Defense Strategy

We will conduct network-centric operations that integrate compatible information and communications systems, usable data, and flexible command and control constructs.

Beyond battlespace operations, a network-centric force can increase the speed and effectiveness across all military operations, intelligence functions, and business processes...

Transforming to a network-centric force requires fundamental changes in process, policy, and culture.

Transform to a Network Centric Force



National Military Strategy

...creation of a collaborative information environment that facilitates information sharing, effective synchronization, and execution of simultaneous operations... on the part of all defense policymakers, warfighters and personnel.

Facilitate Information Sharing

Context for Net-Centric Operations

“Uncertainty is the defining characteristic of today’s strategic environment.”
(National Defense Strategy)

Challenge – UNCERTAINTY

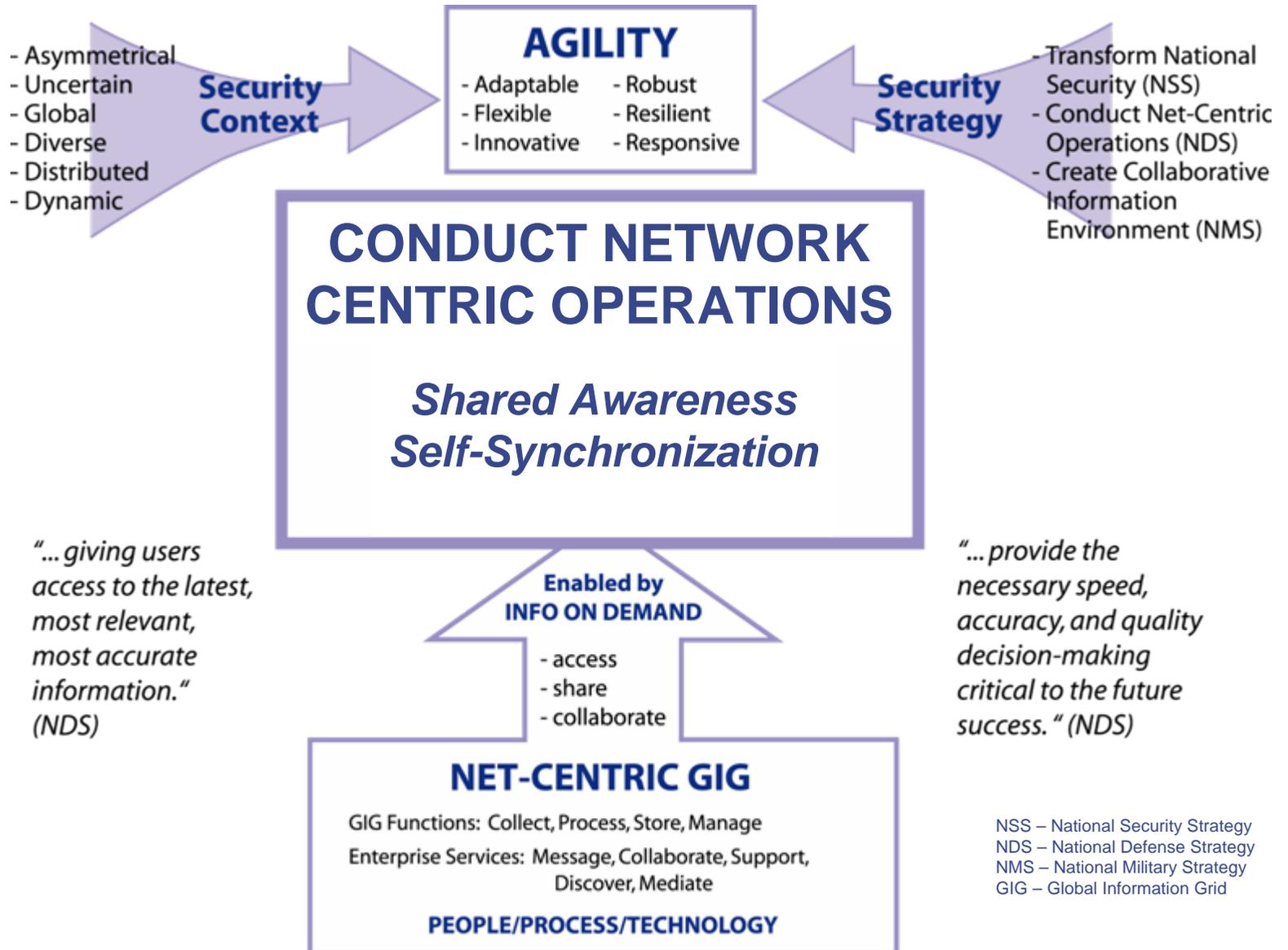
- Leave behind the reasonable predictability of the past
- Adjust to an era of surprise and uncertainty

“We have set about making US forces more AGILE and more expeditionary.”
(Quadrennial Defense Review)

Response – AGILITY

- Enterprise-wide: Battlefield Applications; Defense Operations; Intelligence Functions; Business Processes
- Capabilities Based: Access, Share, Collaborate
- Fundamental Changes: Process, Policy, Culture
- Emphasis Shift: From moving the user to the data – to moving data to the user

Basic Principles of Network Centric Operations



Sources of Agility

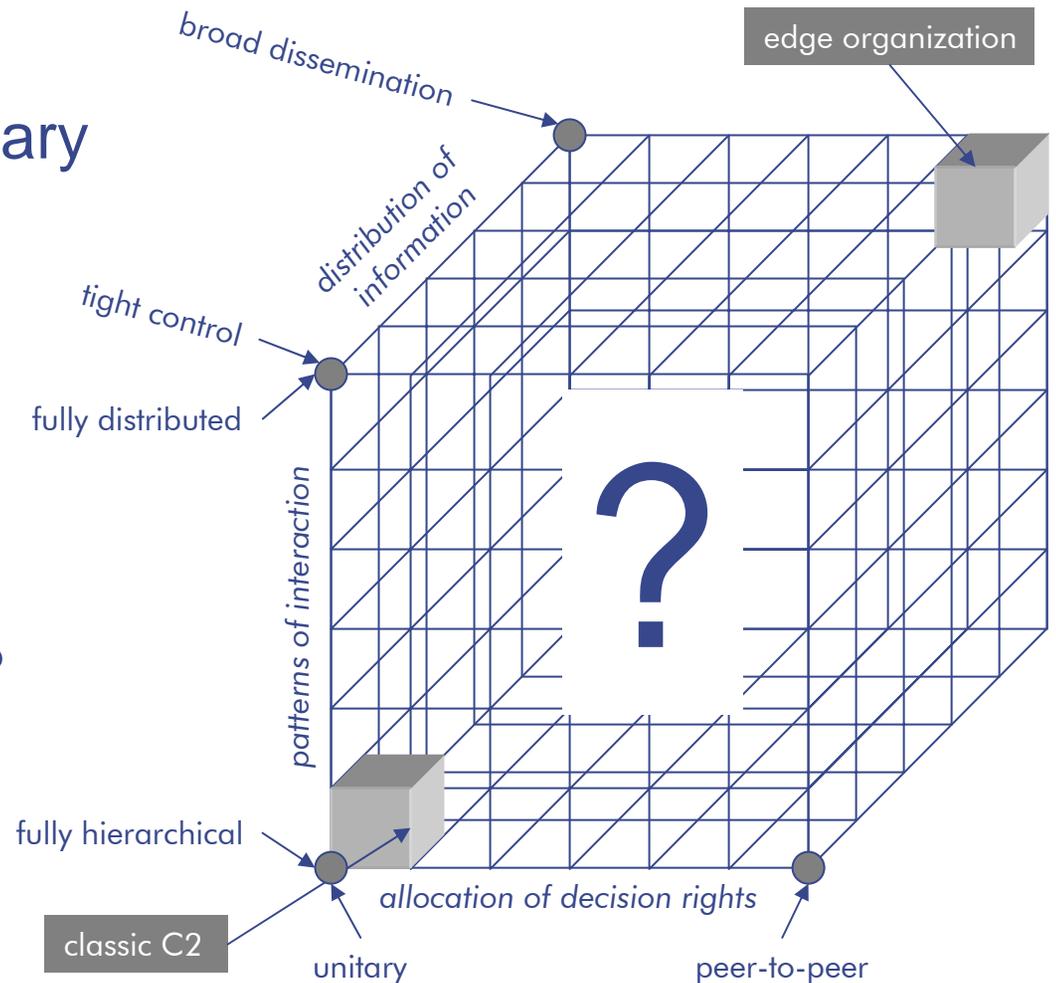
- Agile People
- Agile Systems
- Agile Material
- Agile C2
 - Organizations
 - Processes
- Requires Power to the Edge – Both Means and Opportunity
 - Information Needed to Understand the Situation
 - Authorities Needed to Take Action
 - Resources to Accomplish the Task at Hand
- Perhaps New Terminology: Focus & Convergence

C2 Approach Space

For 21st Century Civil-Military
Multi-National Coalitions

How should we:

Allocate Decision Rights?
Disseminate Information?
Interact with one another?



A Network-Centric Information Environment

“I can get the information and expertise I need”

When I need it



Where I need it



How I need it



“Uncertainty is the defining characteristic of today’s strategic environment”

National Defense Strategy

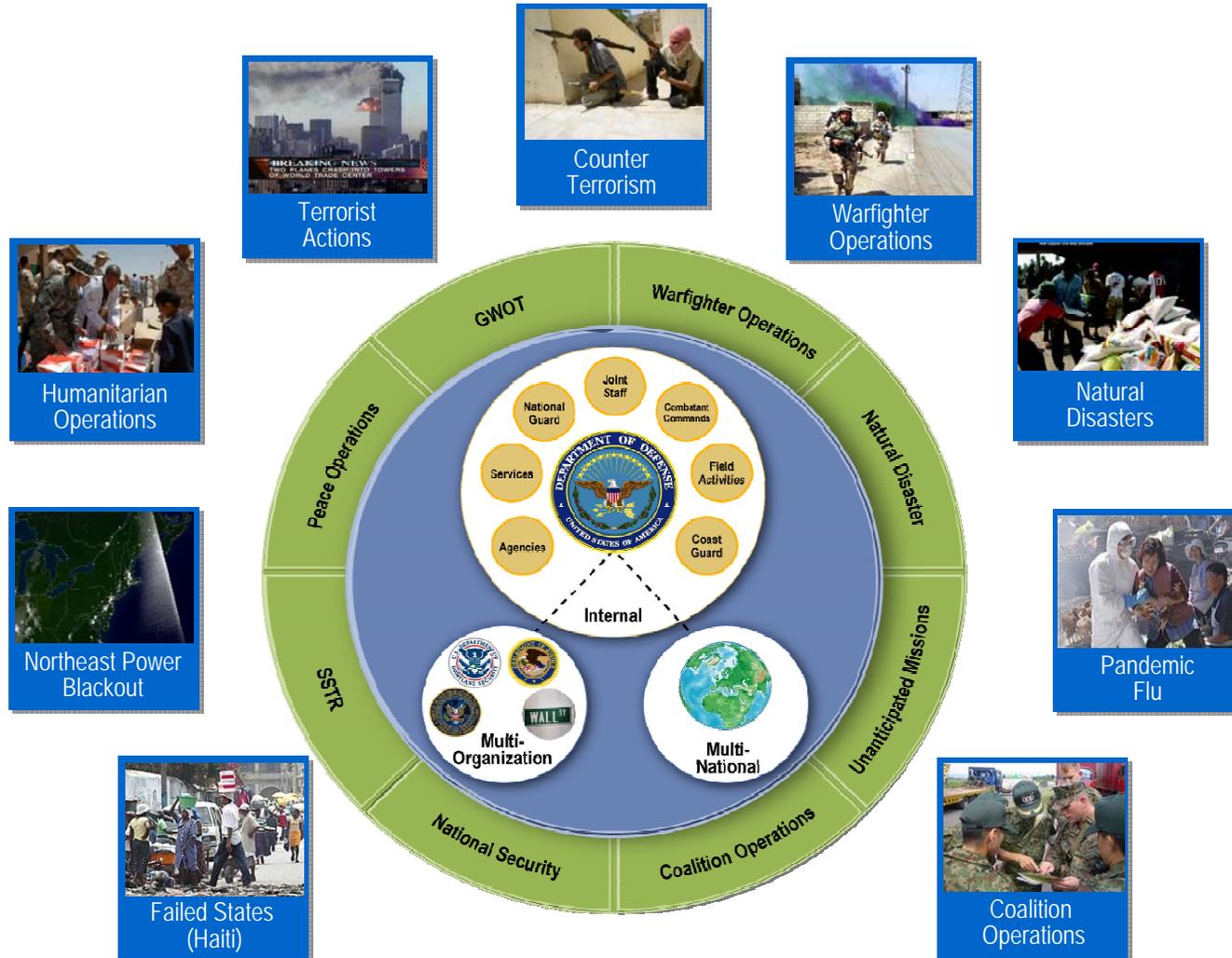
“...focus on providing the tip of the spear with the information and actionable knowledge to determine the best course of action...”

*MG Peter W. Chiarelli
CG, 1st Cavalry Division*

Better Decisions Faster -- Decisive Actions Sooner

Information Sharing

A Simple Concept, A Challenging Task



Unclassified Information Sharing

Regarding support for PACOM efforts responding to 27 May 06 Indonesia Earthquake:

“JFCOM will do whatever it takes to support current operations in this area. In the mid term **we need to figure out how to disseminate unclassified data with the same priority we do classified data** - perhaps more given the complexity of the long war and our need to communicate with non-traditional actors. It is key to how we interact with other nations, OGAs, IOs, and NGOs at all levels of conflict. Let’s work together to fix this shortfall with policy, technology, and processes that support rather than present obstacles. “

General Lance Smith
Commander, U.S. Joint Forces Command
29 May 2006

Unclassified Information Sharing

- DoD Enterprise as part of global information ecosystem
- Can't achieve social, political and economic goals for which military forces are committed without effective engagement with civil partners
- Not a nice-to-have adjunct to kinetic warfare but a core element for eventual success

Unclassified Information Sharing

- Strong Angel III Demonstration
- Value to disaster response community
 - Entrepreneurial approach to developing new capabilities
 - Application to Several DoD missions
 - Humanitarian Assistance and Disaster Relief (HADR)
 - Stability, Security, Transition, and Reconstruction (SSTR)
 - Building Partner Capacity (BPC)
 - Results and Lessons
- Need for better unclassified information sharing
 - Networking challenges: IT and social issues
 - Hastily Formed Networks
 - Trusted and desirable content
- Way Ahead
 - .org or .net solution
 - Other activities

Unclassified Information Sharing

Five parallel approaches needed

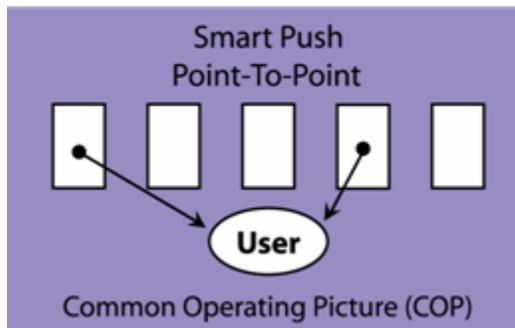
1. Develop capabilities to communicate, collaborate, translate and engage effectively
 - Outside boundaries of military networks
2. Keep building social networks
3. Institutionalize CONOPS, procedures, doctrine, policies
4. Refine legal definitions
5. Make funds available for rapid reaction

An Information Age Approach to Information

Fundamental Shift:

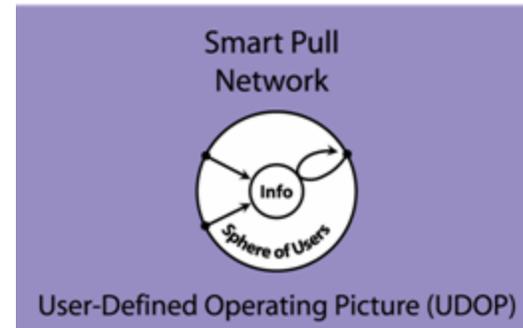
- Requires ENTERPRISE, not stovepipes
- Requires ACCESS, not exclusivity
- Requires TRUST
 - Trust in the System (availability)
 - Trust in the Information (assurability)
 - Trust in the Participants (identity)

Today's Approach: Segregated Stovepipes



User "gets what he gets"

Transformed Approach: Shared Space

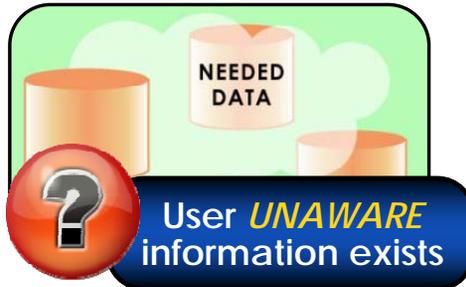


*User "takes what he needs" and
"contributes what he knows"*

Confront Uncertainty with Agility

Data Strategy

Challenges



Goals

Visible



Actions

- Advertise Information
- “Tag” Data



Accessible



- Web Enable Sources
- Remove Impediments
- “Need to Share”



Understandable



- Shared Vocabularies
- Communities of Interest

Securing the Information Environment

Confronting a Persistent Adversary

▪ **The Cyber Threat:**

- **Unconstrained by borders / boundaries**
- Multiple paths of attack – little / no indications or warning
 - **Huge increases in targeted incidents on the Internet**

▪ **The Aggressors:**

- **Responsive to our defensive measures**
- Elusive, innovative - improving their command & control
 - **Increasingly immune, adaptive, enduring**

▪ **The Target:**

- **Information – more valuable / profitable**
- Personal, business & govt. data/intellectual property at risk
 - **Data theft, identity theft, loss, fraud, and deception**

Sharing Information

Fused OPINTEL + Civilian Information

Communities of Interest – Maritime Domain Awareness

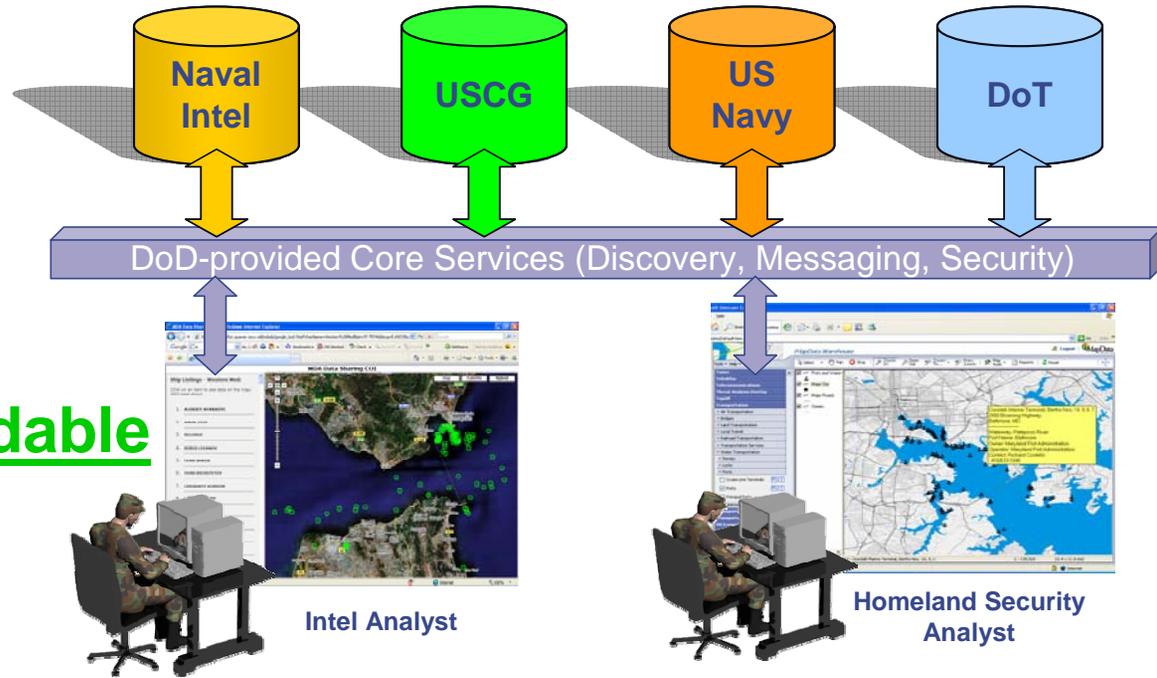
Eight Month Pilot Effort...

- Sources tagged
- Discoverable metadata
- Common vocabulary
- Shared information
- Web services
- User portals

Visible

Accessible

Understandable



Cross-Agency Info Sharing is Happening Today!

Enterprise Security Solutions

Need to move to Mission Assurance

Mission Assurance:

Allow leaders to complete missions under any threats

– **Accelerate Network Defense Initiatives**

- Deploying PKI / CAC, patch management, host-based security

– **Cross-Domain Solutions**

- Aligning policies, processes, governance to drive assured sharing

– **Certification & Accreditation**

- Intel and DoD working together to transform / integrate processes

– **GIG Info Assurance Initiative (GIAP)**

- Managing IA as a capability across the enterprise

– **Protecting Data At Rest (DAR)**

- #1 concern among top security issues (2006 FBI survey)

Summary

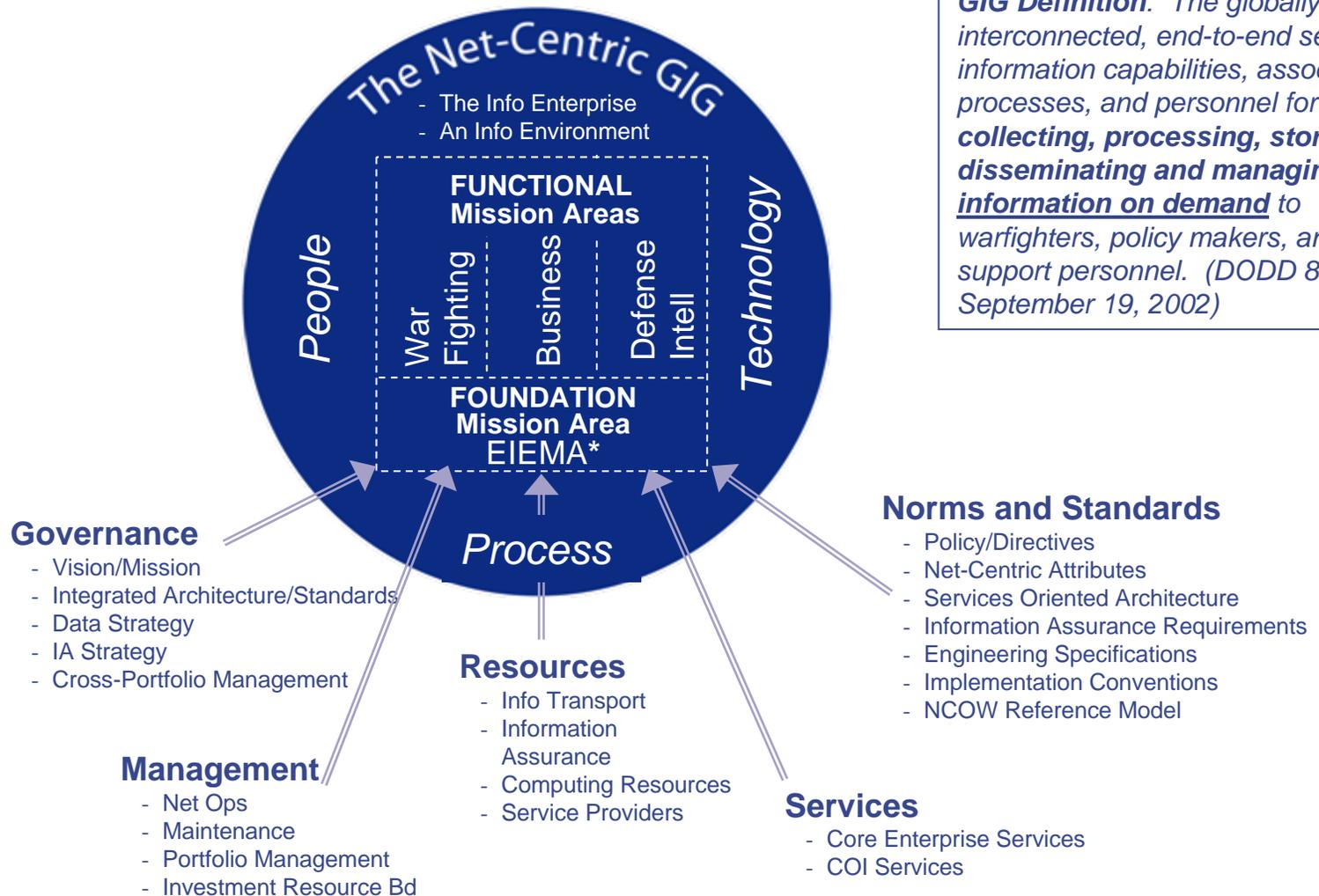
- NCO is delivering today
- Challenges Remain
- On the Critical Path
 - We must be able to share unclassified info outside DoD

Suggest the following slides are not needed

It would be better to spend more time on the above and to illustrate with examples from Iraq, Tsunami, Katrina, etc

The Net-Centric Global Information Grid (GIG)

GIG Definition: *The globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for **collecting, processing, storing, disseminating and managing information on demand** to warfighters, policy makers, and support personnel. (DODD 8100.1 September 19, 2002)*



*EIEMA – Enterprise Information Environment Mission Area

Elements of the Global Information Grid

- Core GIG
- Access Layer
- Tactical Edge

Information Transport

Objective - Provide access to and movement of information regardless of time, location, or disposition

Programs

- **Global Information Grid – DISN Core:**
 - Transforms Defense Information System Network (DISN) capabilities (capacity/availability)
 - Connects fixed locations to each other (but does not reach individual users at the tactical edge)
- **Transformational Satellite (TSAT):**
 - Connects mobile groups of users to each other and to fixed locations
 - Extends reach to individual users at the tactical edge
- **Joint Tactical Radio System (JTRS):**
 - Connects individual users within a group of mobile users
 - Provides network entry device for individual users at the tactical edge
- **Teleports:**
 - Provides a gateway between TSAT and DISN Core
- **Spectrum Management**
 - Ensures access to the airwaves

Pace of DoD Acquisition vs Technology Velocity

- Moore's Law vs FYDP Timelines
- COTS Incorporation
- Spiral Development
- Managed Services
- Configuration Control, Training and Personnel

The New Business Model: Implications for Industry

Managed Services and Service Oriented Architecture

CHANGING FROM THIS:

Build a Platform →
Buy “Things” →
Own It →
Application Focused →
Closed Systems →
Proprietary Solutions →
Stovepipes →
Pre-Engineered Interfaces →
Info Assurance After-the-Fact →
Password Access →

CHANGING TO THIS:

Create an Environment
Purchase Managed Services
Use It
Data Driven
Open Service Oriented Architectures
Common Standards
Enterprise
Accommodate Unanticipated Users
Information Assurance Baked-In
Attribute-Based Access

CONFRONT UNCERTAINTY WITH AGILITY

Supply Chain Issues

- In a global environment, adversary access and opportunity to do harm pose significant risk to our critical ICT infrastructure
 - Global supply chain provides effective avenues to cause harm over the **lifecycle of ICT products and services** that make up USG networks
- Require a multi-faceted risk mitigation strategy to reduce risk throughout the ICT lifecycle
 - most vulnerable points often reside with services and functions providing access rather than with physical infrastructure assets
 - The strategy emphasizes security across entire product lifecycle
- Important component of risk mitigation is robust coordinated research and development agenda
 - Enhance the U.S. state of the art in building and identifying trusted hardware and software - IT assurance
 - Build closer relationships with the private sector and academia towards diagnostic IT capabilities
 - Identify next generation tools and methods to limit access and opportunity and assure the integrity of ICT products and services