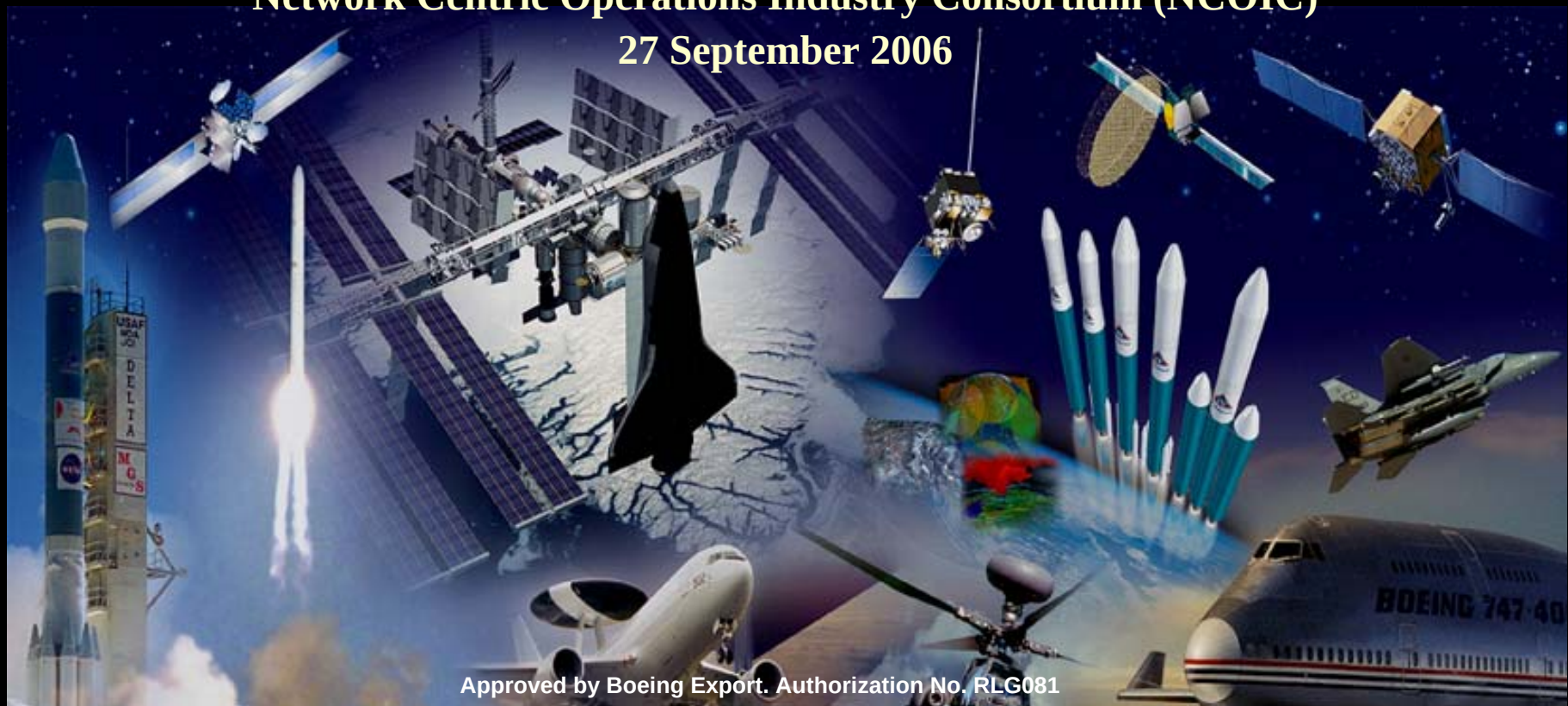
The Net-Enabled Future:

An OCTANe Discussion Panel Topic

Sheryl Sizelove, The Boeing Company

Network Centric Operations Industry Consortium (NCOIC)

27 September 2006



What is Network Centric Operations (NCO)?

… an Information Age Transformation

Getting the Right Information to only the Right People, at the Right Place and Time…

It's all about being More Effective

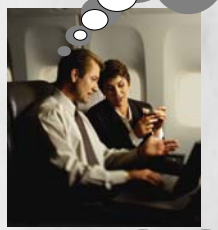
Fundamental Information Needs

- Knowledge Learning
- Comfort, Pleasure
- Decision Support
- Situational Control
- Situational Awareness
- Safety/Protection

Where am I?
Where are my friends?
Where is the enemy?
What is the enemy's intent?

Where am I?
Where are the airplanes?
What is the weather enroute?
What is the best route?

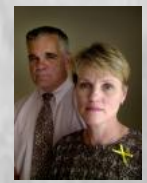
Where am I?
When will I arrive?
What is my schedule?



Where am I?
Where are the dangers?
Where are my compatriots?
What are the hazards?

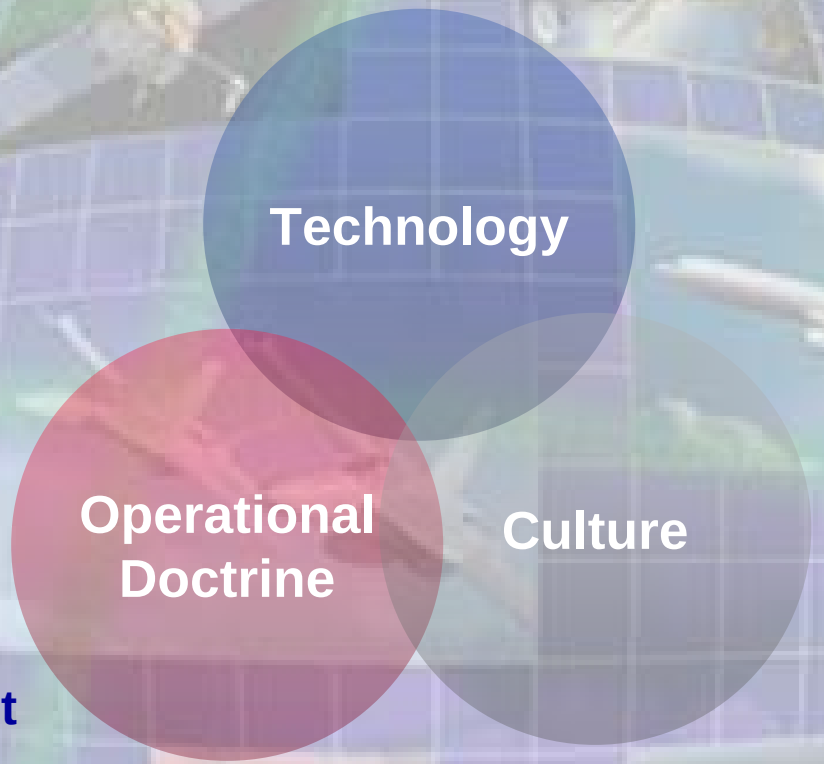
Where am I?
What is the weather?
What should I apply to my crops?
How are the fields?

Where are we?
Where are the kids?



Three Major Parts of NCO

New capabilities and technologies that enable communication, information sharing and collaboration within and among communities



Describes how we organize and the protocol that defines how we Interact in a net-enabled environment

Our willingness to change, trust, delegate and enable

NCO characterizes new operational doctrine that leverages new capabilities, organizational structures and behaviors

Issues in Achieving NCO

- "Stovepipe" system design limits System-of-System capabilities
  - Comms for existing systems are often point-to-point (non-networked)
  - Transition from Integrated Performance-Oriented Systems to Service-Oriented Architectures (SOA)
- Security and Concerns over Control of Data
  - Increasingly Joint & Coalition military operations
  - Increasingly involving Civilian and Non-Government Agencies
- Limited Budgets: Having to "Do More with Less"
- Schedules: Too short to implement; Too long to obtain
- Cultural Resistance
  - "That's Not How We Do Things"
  - "Turf" concerns
  - Fear of Change

Technology is a Challenge, but Cultural Change is a Bigger Challenge!

NCOIC Consortium

Vision:

Industry working together with our customers to provide a network centric environment where all classes of information systems interoperate by integrating existing and emerging open standards into a common evolving global framework that employs a common set of principles and processes.

- **Primary tenets of the Consortium's vision:**
  - **Work to identify and develop a Network Centric environment**
  - **Provide assured technical interoperability**
  - **Embrace, enhance, and encourage open standards**
  - **Establish and educate on common principles and processes**

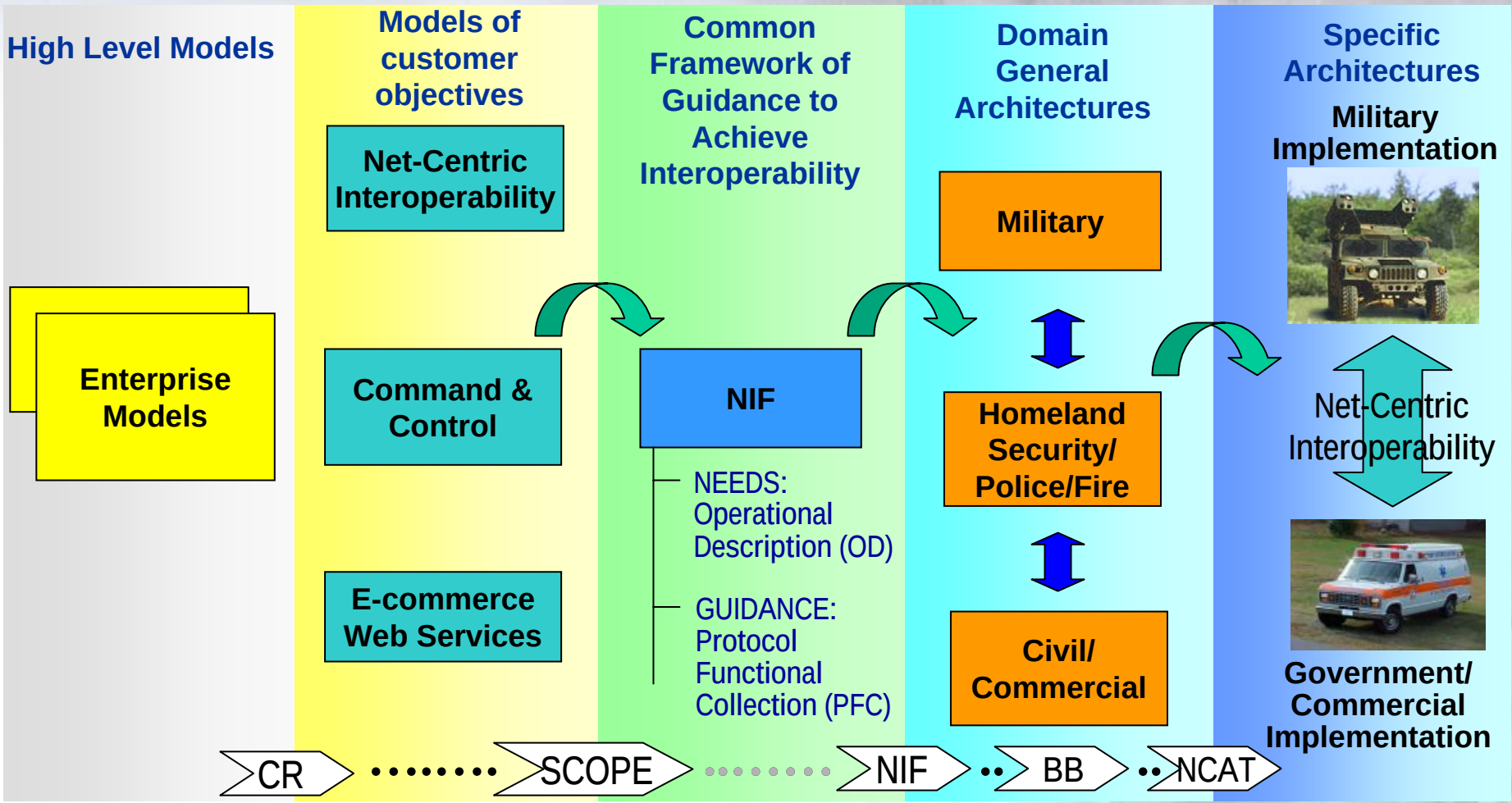
Mission:

Facilitate global realization of the benefit inherent in Network Centric Operations. We seek to enable continuously increasing levels of interoperability across the spectrum of joint, interagency, intergovermental, and multinational industrial and commercial operations. We will execute this mission in good faith as a global organization with membership open to all enterprises in quest of applying the vast potential of network centric technology to the operational challenges faced by our nations and their citizens.

Currently 80 Member Companies in the NCOIC

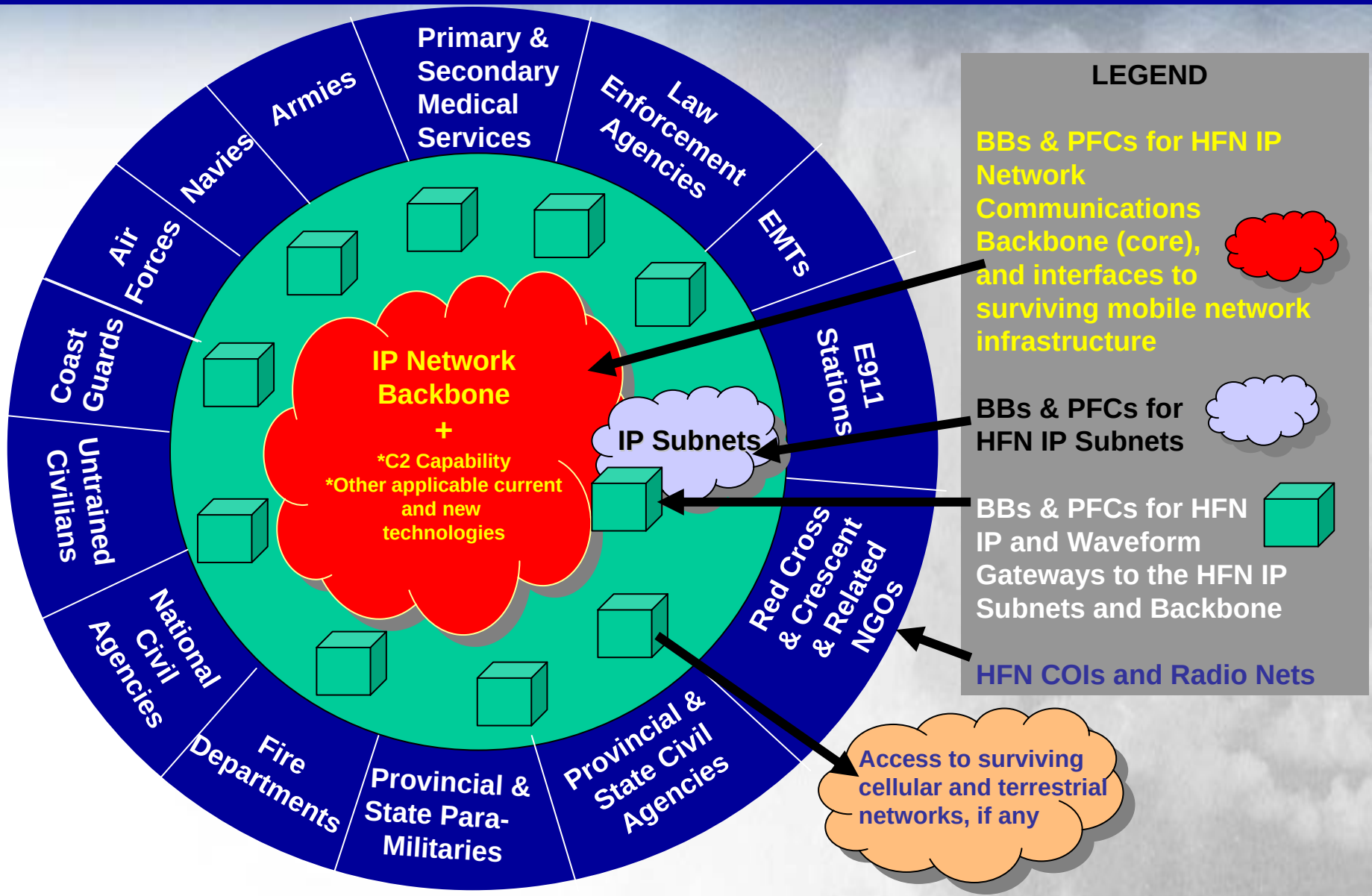
Just a few of the names that you might recognize…

NCOIC Technical Deliverables



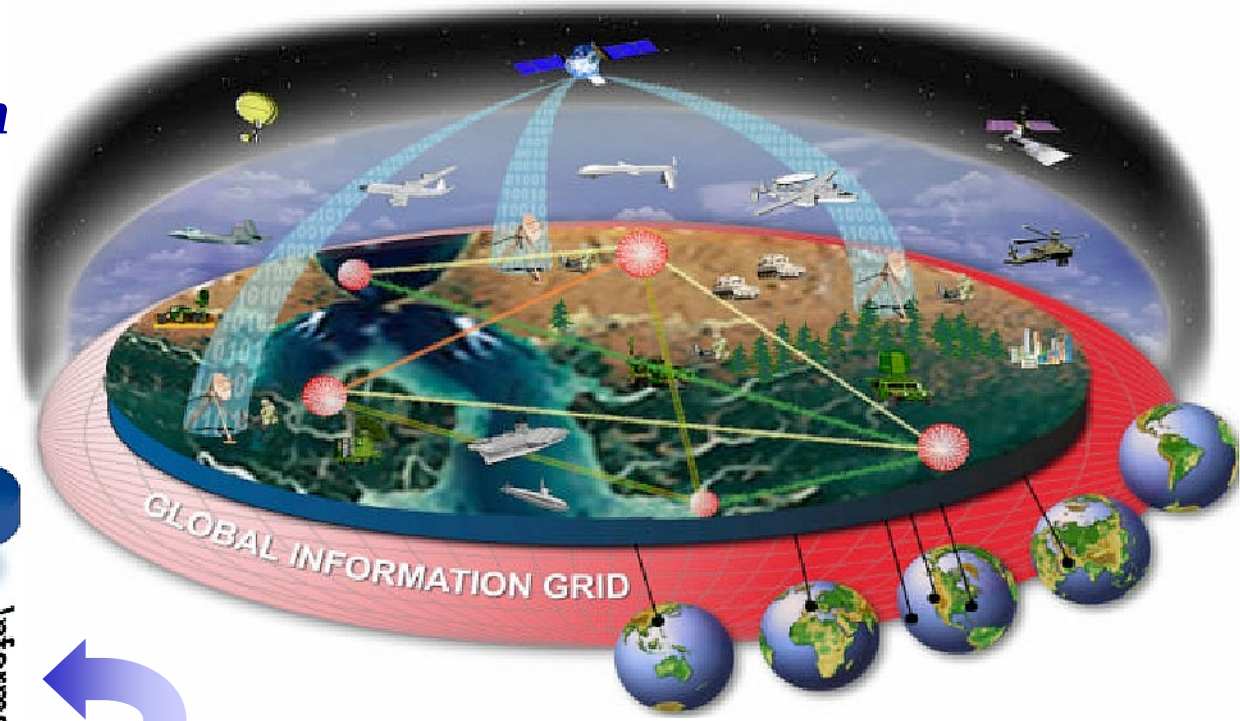
NCOIC tools work together to assist in achieving interoperable systems

For Example: Mobile Emergency Communications Interoperability after a Complex Humanitarian Disaster



The GIG: Goal of the U.S. Department of Defense

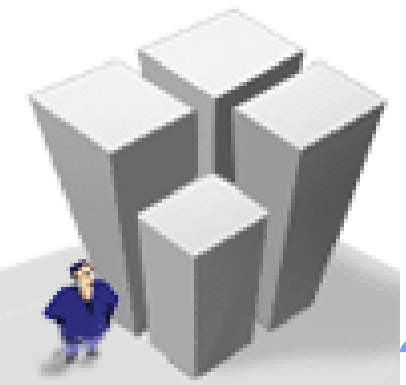
The Global Information Grid (GIG)



The GIG Enterprise Services (GES), supported by the core Net-Centric Enterprise Services *(NCES: Discovery, Mediation, Collaboration, Messaging, Enterprise Service Management, Application, Storage, User Assistant, IA/Security)*

Net-Centric Future

NCOIC



Stovepiped Systems, Point-to-Point Networks

BACKUP

Network Security Challenges

Description of Challenge	***Candidate Solution(s)***
• Packet Eavesdropping & Spoofing ("Man In The Middle" Attack)	• IPSECv6: Encapsulated Security Payload (ESP) with Authentication Header (AH), Quantum Key Distribution (QKD)
• Denial of Service (DoS) Attack (and Distributed DoS or DDoS)	• Multiprotocol Label Switching (MPLS)
• "Need To Share" rather than need-to-know in a mixed security level environment requiring high assurance	• Multiple Independent Levels of Security (MILS) with Role-Based Access Control (RBAC), follow DoD Information Assurance Certification and Accreditation Process (DIACAP)
• Polymorphic Worms and other increasingly-sophisticated attack	• IPv6, Defense-in-Depth, Intelligent Software Agents in SW Guards

New Security Headaches: Staying Ahead of the "Black-Hatters"