National Defense Industrial Association (NDIA) Armaments Technology Seminar & Exhibition

Leveraging Enabling IT Technologies for "The Home and Away Game"

Panel Discussion on Adapting Lethality for Homeland Defense/Security

Presented by: Angela M. Messer
Principal, Booz Allen Hamilton
McLean, VA
June 15, 2005

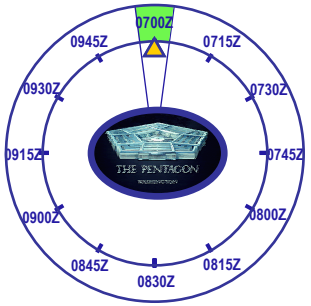
Discussions topics on leveraging enabling IT technologies for homeland defense and homeland security

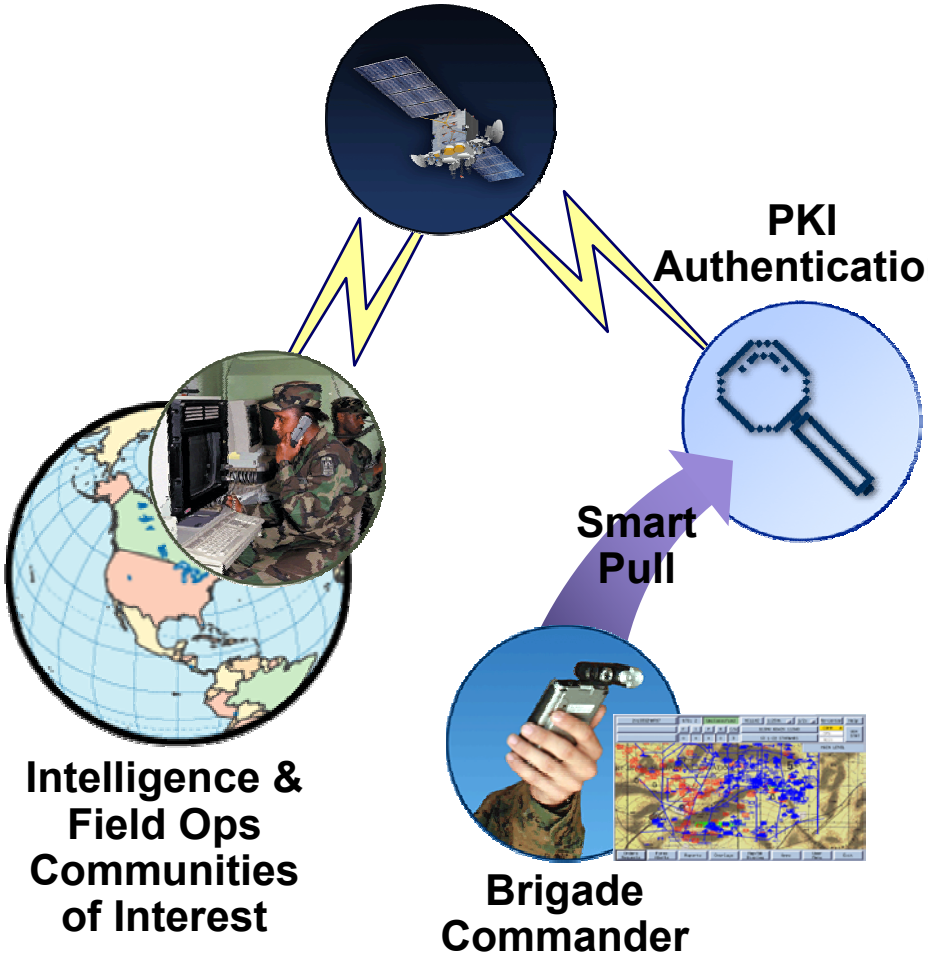
- The need for the 'NET' and a net-centric environment to connect systems, information and users
- The power of the enabling technologies for the 'home and away games'
  - Communications
  - Data and information sharing
  - Net-centric capabilities
- 4 Case studies
  - 'Home Game' -- National Guard
  - 'Home Game and Away Game' -- DoD Biometrics Management Office and the Biometrics Fusion Center
  - 'Away Game' efforts that have potential to impact the 'Home Game' -- DCGS-Army and JIAPC
- Critical success factors

Future Combat Scenario

- Power of the ‘Net’
- Information sharing capabilities
- Could we apply this scenario to the HLS/HLD environment?

0700Z: Brigade Commander Logs Into "My GIG"

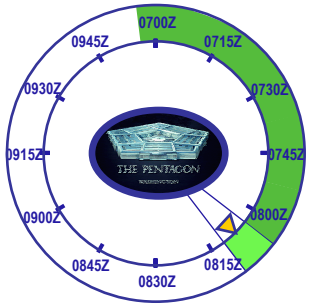


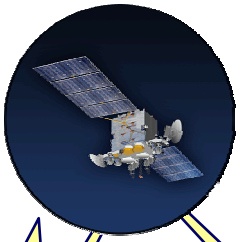


- Logs into the GIG directly via a portable device
- Commander's Identity and device are identified and registered to the GIG
- Updates Subscription services, add new COI(s) and sets up alerts.
- Reviews published reports

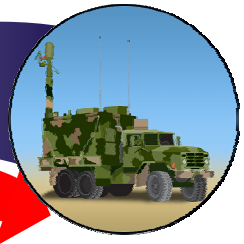
Afghanistan

0810Z: Recon Team Picks Up SIGINT



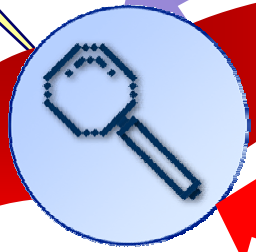


"Possible Enemy Produced Armored Vehicles"



Alert Message

Tactical Intelligence Unit



Alert Message

Intelligence & Field Ops Communities of Interest

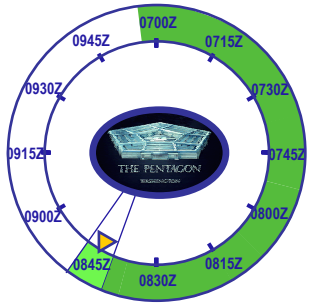
Brigade Commander

SIGINT

Possible enemy emitter detected

Afghanistan

0845Z: Brigade commander quickly establishes task force and COI – inviting participants and including needed assets



Strike Package

"Stand By"

UAV

"Eyes on target"

Establishes COI

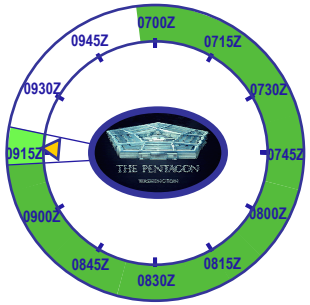
Intelligence & Field Ops Communities of Interest

Brigade Commander

Recon Team

Afghanistan

0917Z: Target Identified



DIA Analyst: "…unlikely to be armored division; possible deception"

Reaching back to subject matter experts

Strike Package

Coalition Partners

"No enemy sighted in area past 30 days"

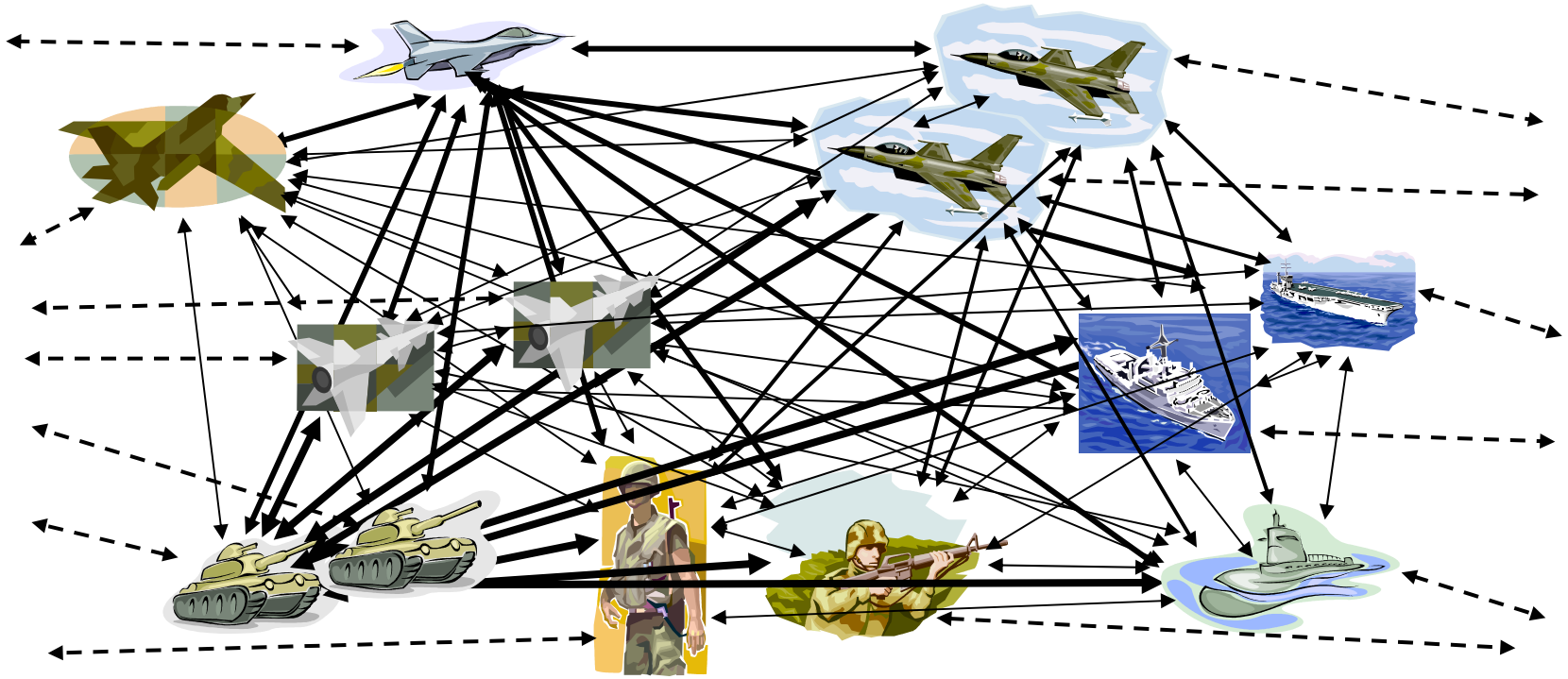
Video of vehicle convoy

Recon Team

"I see two Red Cross Trucks"

Afghanistan

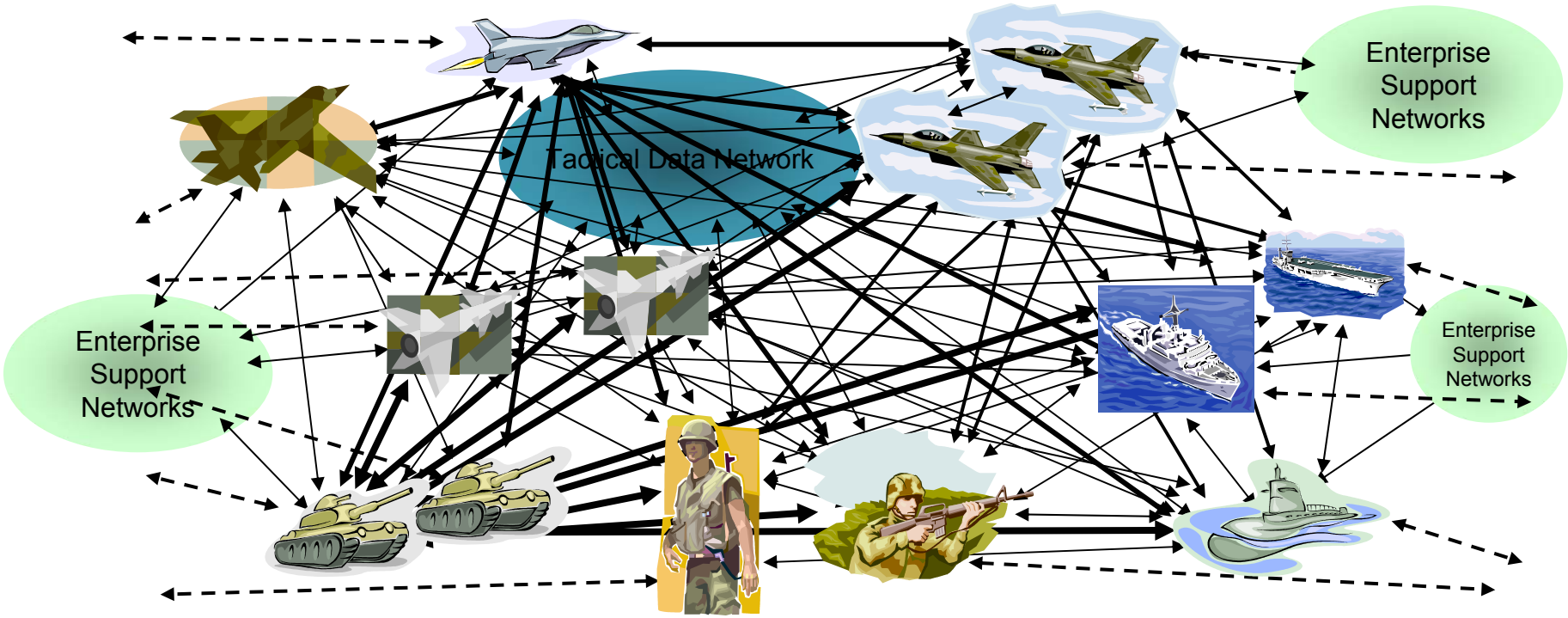
The possible connections between platforms, people and systems required for NCW is typical of what analysts call an "n^2" problem …



15 interfaces

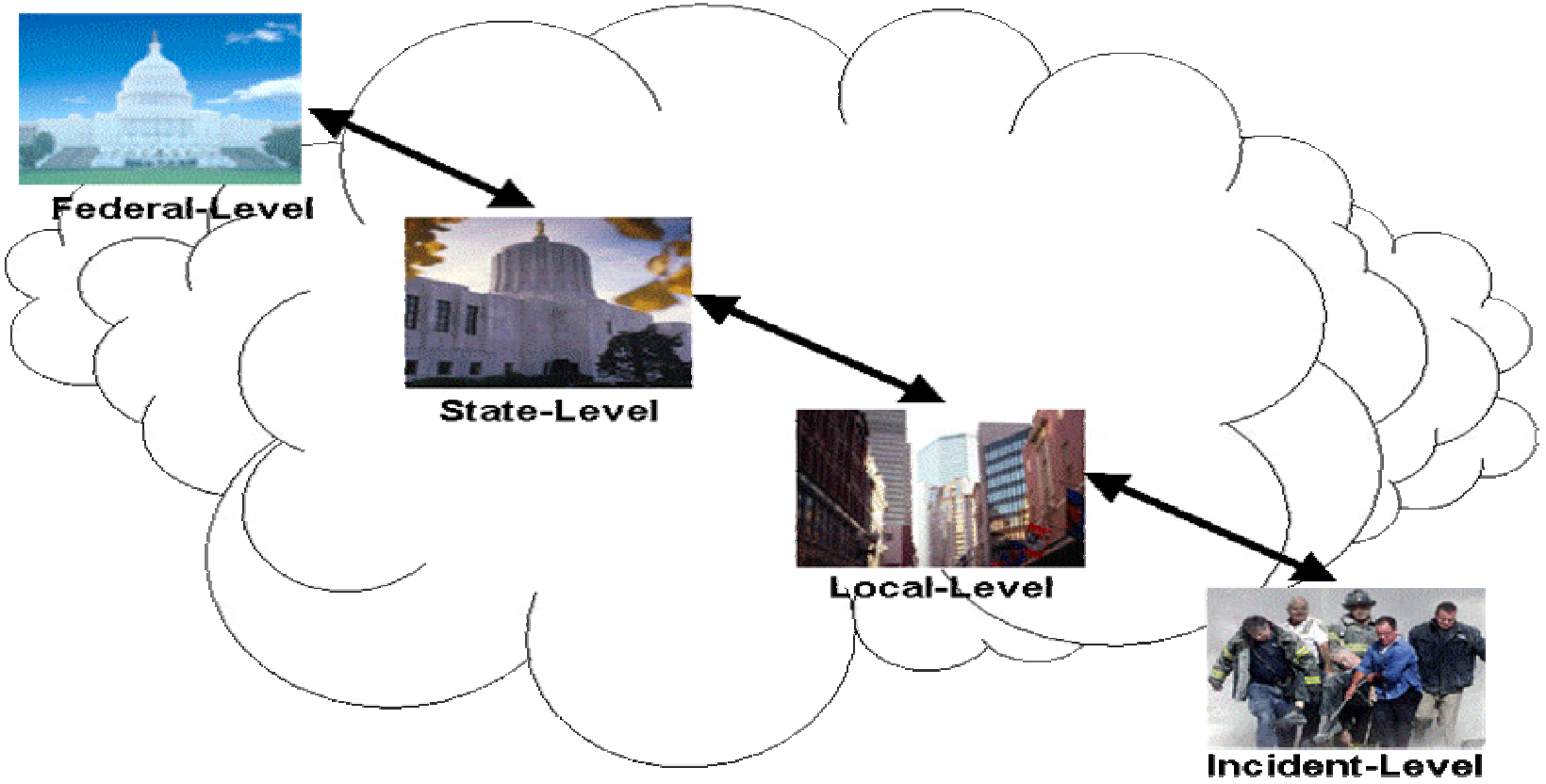
… where the difficulty climbs exponentially with each new component; "n^2" problems don't scale well

The term “net-centric” is intended to position “the network” as the source and destination of information and is critical in enabling information sharing …



… but effecting this transformation requires wholesale changes in technology, policy, and culture

For the 'Home Game" -- the complexities in HLS/HLD are compounded by the number of stakeholders at the local, state, regional and federal level – which requires enhanced training, equipment, information exchange and sharing, and knowledge sharing capabilities



Complexity increases with regional and national scenarios

The Mega Trends in enabling technologies --- Wave One and Two initiatives are exponentially fueling information growth and access, generating the need for Wave Three products and services to exploit this information

1 Wave One: Computing/Processing (1960s-1980s)

- **Technology Catalyst**
  - Microprocessor/WINTEL
- **Characteristics**
  - Standardized
  - Commoditized
- **Business Benefit**
  - Desktop applications
  - Decentralized processing
- **Key Challenges**
  - IT as largest capital expense/TCO
  - Linkage to productivity

2 Wave Two: Communication/Networking (1980s-2000s)

- **Technology Catalyst**
  - TCP/IP, Ethernet
  - HTML
- **Characteristics**
  - Distributed
  - Open
- **Business Benefit**
  - Increased collaboration
  - Greater information access
- **Key Challenges**
  - Security
  - Impact on business model

3 Wave Three: Content & Data Management (2000-2010s)

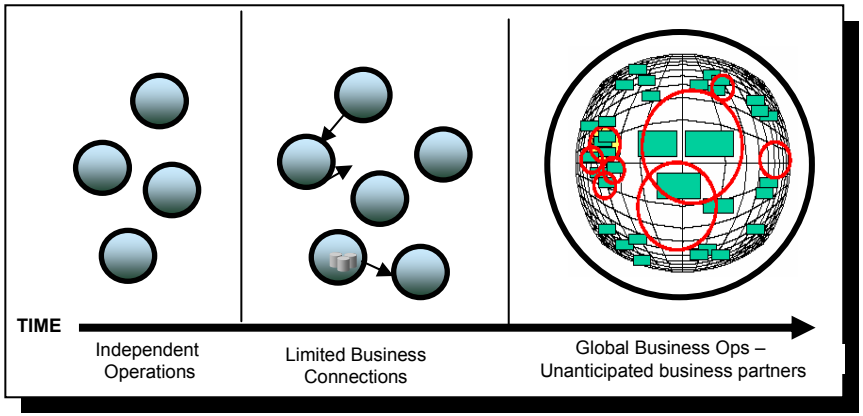
- **Technology Catalyst**
  - XML
- **Characteristics**
  - Standardized
  - Integrated
- **Business Benefit**
  - Real-Time Integrated Enterprise
  - Turing Data into Actionable Knowledge
- **Key Challenges**
  - Information Management
  - Cost and Complexity
  - Impact on business model
  - Security

SOA and web service technologies are becoming the next IT revolution, helping organizations align their software applications with business and mission requirements

Technology Evolution

	1960's - 1980's	1980's	Early 1990's	Mid 1990's	2000's
Approach	Mainframe	Mainframe	Client Server	Web	SOA
Architecture	1 Tier	1 Tier	2 Tier (Server, Application)	3 Tier (Database, Server, Client)	Service Oriented
Business Motivation	Initial Automation	Initial Desktop Computing Power	Greater Desktop Computing Power	eBusiness	Business Agility

Business Model Evolution



Terminology Evolution

- Microsoft coined the term "Web services" in June 2000, when the company introduced Web services as a key component of its .Net initiative, a broad new vision for embracing the Internet in the development, engineering and use of software.
- Gartner coined the term "Service Oriented Architecture" in the late 90's to describe a component-based distributed computing environment
- Developers use XML tags to describe individual pieces of data, forming XML text-based documents that can be processed on any platform
- Web services take advantage of object-oriented programming by enabling developers to build applications from existing software components using a modular approach

Case Study #1
Joint CONUS Communications and Support Environment (JCCSE)

"Trusted Information Sharing, Collaboration, and a COP for Homeland Defense and Civil Support (HLD/CS) Missions"

NG Operational Scope (OV-1)

Principal Partners: Combatant Commanders

Federal Defense Missions:
Deployed as part of Joint Task Force

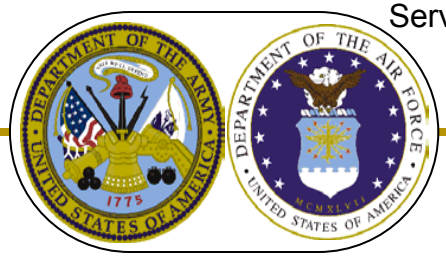
Mobilization

The National Guard

Federal Missions
Long & Short Term Plans
War Planning
Coordination
Common Operating Picture
Situational Awareness

Actions

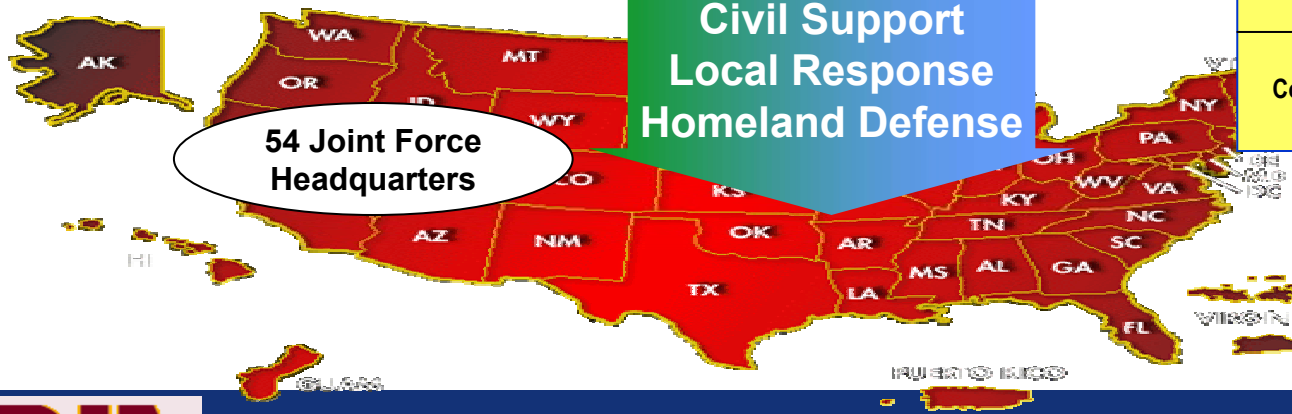
Parent Military Services



"Away Game"

"Home Game"

Civil Support
Local Response
Homeland Defense



54 Joint Force Headquarters

State Missions
Unit Status & Training
HD/MACA Planning
Coordination
Common Operating Picture
Situational Awareness

Actions

Principal Federal Partners

Information Technology Infrastructure based on the Global Information Grid

‘The Home Game’ -- IT Support for Homeland Defense & Civil Support

- Need for a ***collaborative information exchange environment*** for support of inter-agency situational awareness, information sharing, and collaboration requirements, and supported by ***IT capabilities that are simple to deploy and use***

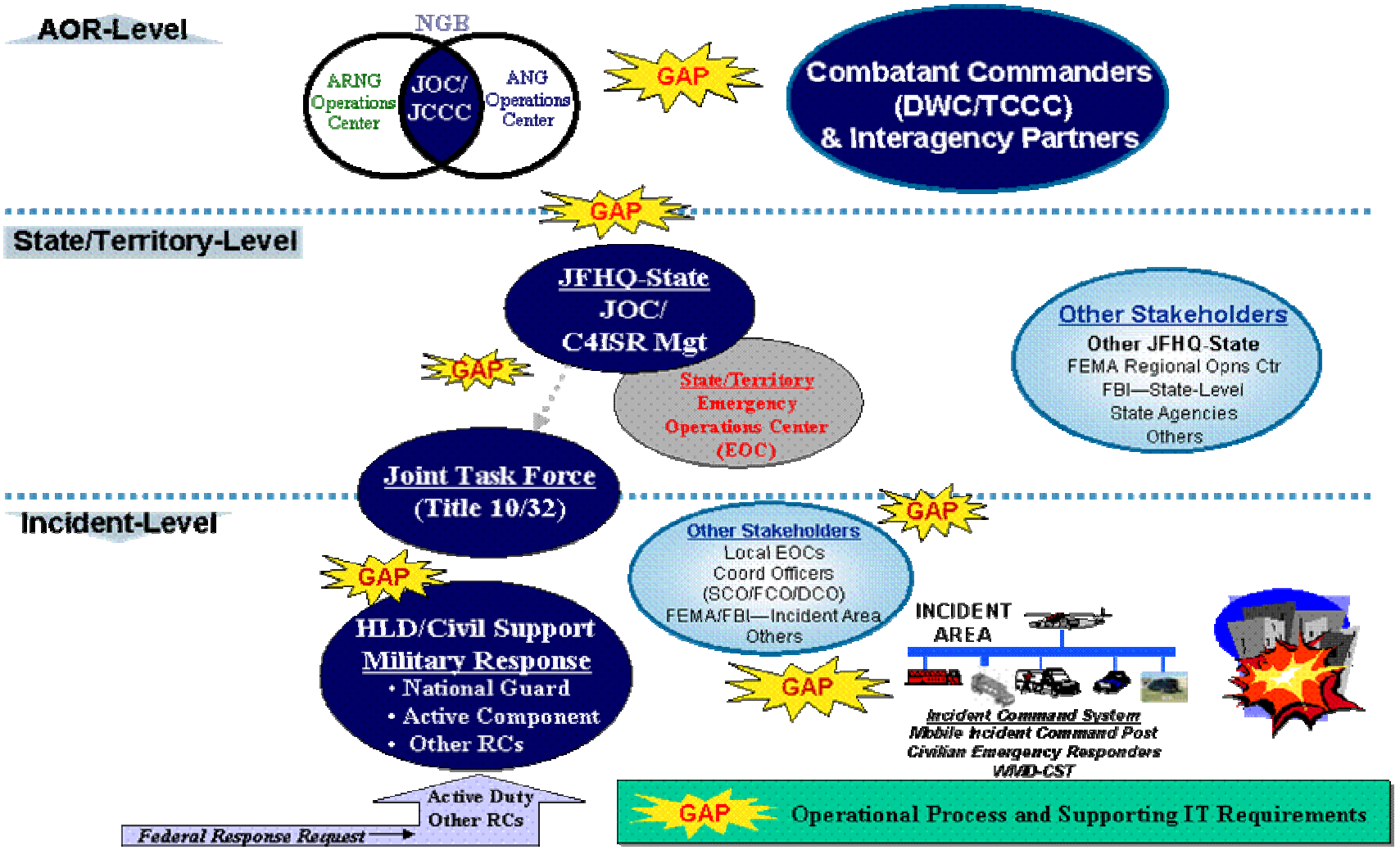
- Need for a ***deployable incident area communications organizations throughout the 54 States/Territories*** with specified capabilities, response times, and readiness standards to ***extend collaborative information exchange capabilities to any incident site***

- Need to develop IT capabilities for ***Title 10/32 dual-hatted Joint Task Force commanders*** and other possible C2 structures employed for Homeland Defense & Security missions

- Need for a ***continuous situational awareness of our IT resources*** so they can be more effectively employed to support users at the National- and State/Territory levels, and incident site

The Joint CONUS Communications Support Environment (JCCSE) construct provides the vision for supporting these requirements

JCCSE Mission Environment leverages wireline and wireless networking, Ka and Ku band satellite, land mobile radio, VPNs, and incident management collaboration/intelligence analysis tools



JCCSE provides information sharing, collaboration, and COP development and sustainment capabilities supporting all levels, including to/from any incident site

JCCSE Definition and Way Ahead

- The JCCSE is an "umbrella" term for the National Guard's (NG's) information technology (IT) support for Homeland Defense and Civil Support (HLD/CS) missions

- JCCSE provides multiple, inter-dependent organizational as well as technology components – both C4ISR and commercial technologies, tailored to support National Guard HLD/CS mission requirements

JCCSE Organizational Components

- **Operations Centers**
  - -- NGB JOC
  - -- JFHQ-State JOCs
- **C4ISR Management**
  - -- NGB Joint C4ISR Coord Ctr (JCCC)
  - -- JFHQ-State J-6 IT Environment Mgt
- **Incident Area Communications**
  - -- JTF Communications Element

JCCSE Infrastructure Components

- **Network and Net-Centric IT Services**
  - -- Leverage GuardNet & ANG Enterprise Net
  - -- Migrate toward DoD Enterprise (e.g., GIG-BE)
- **Incident Area IT Capabilities**
  - -- First Responder Interoperability
  - -- Deployed NG Forces Support
  - -- Reach Back Capabilities
  - -- Other Validated HLD/CS Mission Support

- JCCSE extends inter-agency trusted information sharing and collaboration capabilities to and from the National-level, the 54 States and Territories, and local incident sites

- NGB, in collaboration with COCOMS(s) and all JFHQ-State, takes lead and stands up JCCSE

- JCCSE evolves as part of the larger DoD enterprise, leveraging the GIG and the current infrastructure/infostructure

Case Study #2
DoD
Biometrics Management Office (BMO) and Biometrics Fusion Center (BFC) --

Protecting the Homeland

Protecting the Homeland -- Background on DoD BMO and BFC

- Army CIO/G-6 is DoD Executive Agent for Biometrics and the key architect of DoD biometrics guidance (pursuant to Public Law 106-246 (13 Jul 00))
- DoD Biometrics Management Office (BMO) focus on Policy and Standards has led to significant progress in the DoD biometrics community

- Since 21 Jul 04, the DoD Biometrics Fusion Center (BFC), under the Army CIO/G-6, has been processing, searching, and matching biometric data, primarily fingerprints, to identify national security threats.

- This biometric effort has received extensive support from the Office of the DepSecDef, ASD (HD), ASD (NII), NORTHCOM, National Detainee Reporting Center, Army G-2, Army CIO/G-6, National Ground Intelligence Center, CENTCOM, U.S. Force Protection Initiative, Terrorist Explosives Device Analytical Center, the FBI Criminal Justice Information Services Division, and the FBI Lab.

- As of 9 May 05, the BFC has made 1884 significant matches.

- Elements of the DoD Biometrics enterprise solution, including the DoD Automated Biometric Identification System (ABIS) and Biometric Identification System for Access (BISA), are examples of how biometrics has identified potential national security threats to protect the homeland.

DoD Automated Biometric Identification System (ABIS)

Terrorist/Crime Scenes (Latents – 800)

DoD Organizations

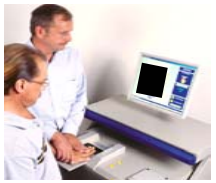
Naval Special Warfare Command Suspects (Ten flat – 125)

BAT – Detainees, Locally Employed Personnel, misc. (Various – 57,000)

Automated, secure linkages planned in 2005

Other Governmental Organizations

1991 PGW EPW (Various – 81,165)



Force Protection Initiative (Ten rolled ~72,363)

DoD Biometrics Fusion Center DoD ABIS

FBI CJIS

Current Biometric Data

Criminal Master File

Operation Enduring Freedom / Operation Iraqi Freedom Persian Gulf War Enemy Prisoners of War Force Protection Initiatives

~49M records of persons arrested in the U.S.

Arrestees in U.S.

National Security Entry/Exit Registration System (Two flat index ~400)

Force Protection Initiative 2 (Ten rolled – 115,893)

Latent Fingerprints – uploaded to AKO for information sharing for key stakeholders

B

Latent prints

AKO-Secure Folders

Latent Upload

Search Results by ISN

Match Notification

CIA

DIA

G-2

State

Other

A

B

A

DoD ABIS

FBI CJIS IAFIS

A	Biometric Data (sent from organization A)
B	Latent print uploaded to AKO

Impact of these enabling IT technologies for HLD/HLS

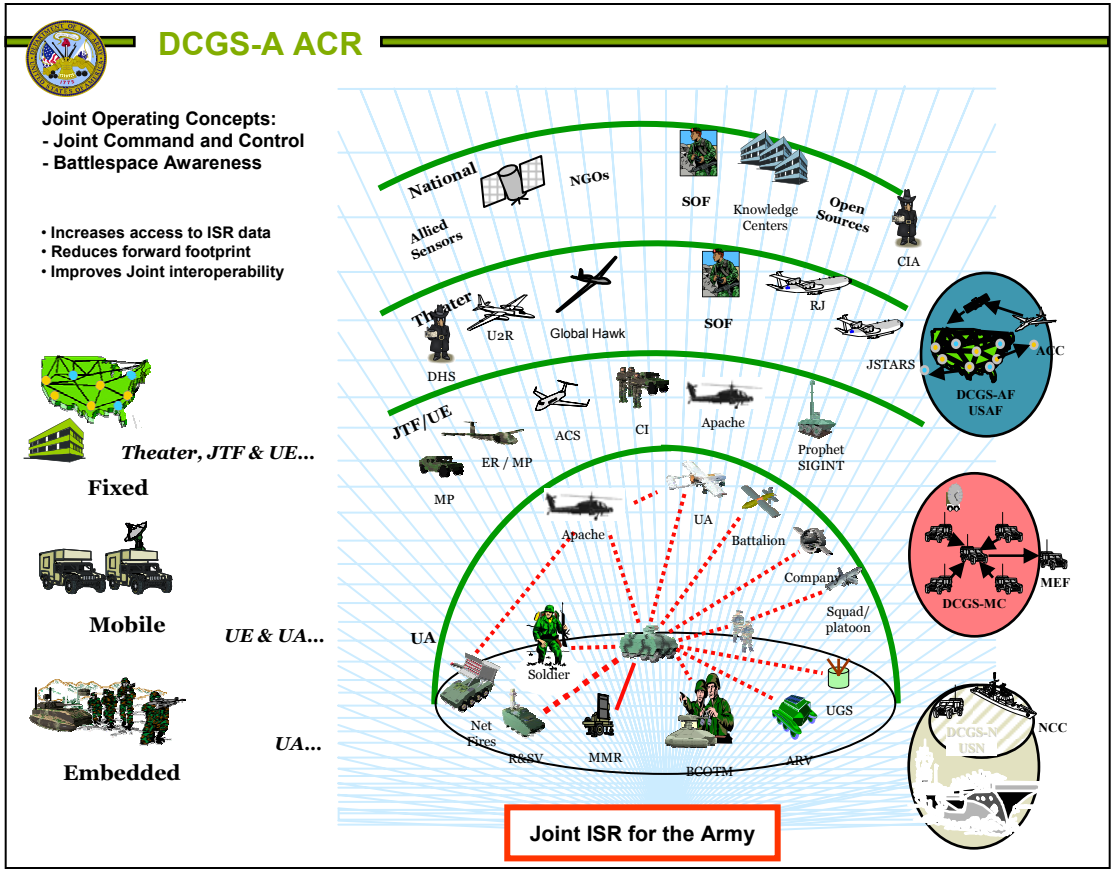
- DoD ABIS has directly aided the warfighter and law enforcement since its inception in Jul 04
  - ABIS has made 1884 significant biometric matches to date (21 Jul 04 – 9 May 05)
  - Matches include suspected bombmakers, passport forger
- ABIS & BISA initiatives will significantly enhance force protection efforts at U.S. installations – at home and abroad
- DoD Biometrics plays a central role for the DoD and USG in identifying potential national security threats

Case Study #3
Distributed Common Ground System Army (DCGS-A)

Situational Awareness for the Warfighter and possibly the HLD/HLS community

DCGS-A Mission and Operational View

- DCGS-A Enables Situation Awareness, Identification and Location of Enemy and Estimates of his Intentions to the Warfighter at All Echelons
- DCGS-A Enables Exploitation and Fusion of Data From Army, Joint, National and Allied Sensors and Sources to Provide the Information Needed by the Warfighter
  - If applied to HLD/HLS, law enforcement and other stakeholders could be sensors and sources of information for the COP
- DCGS-A is the Army component of the DoD DCGS Family of Systems

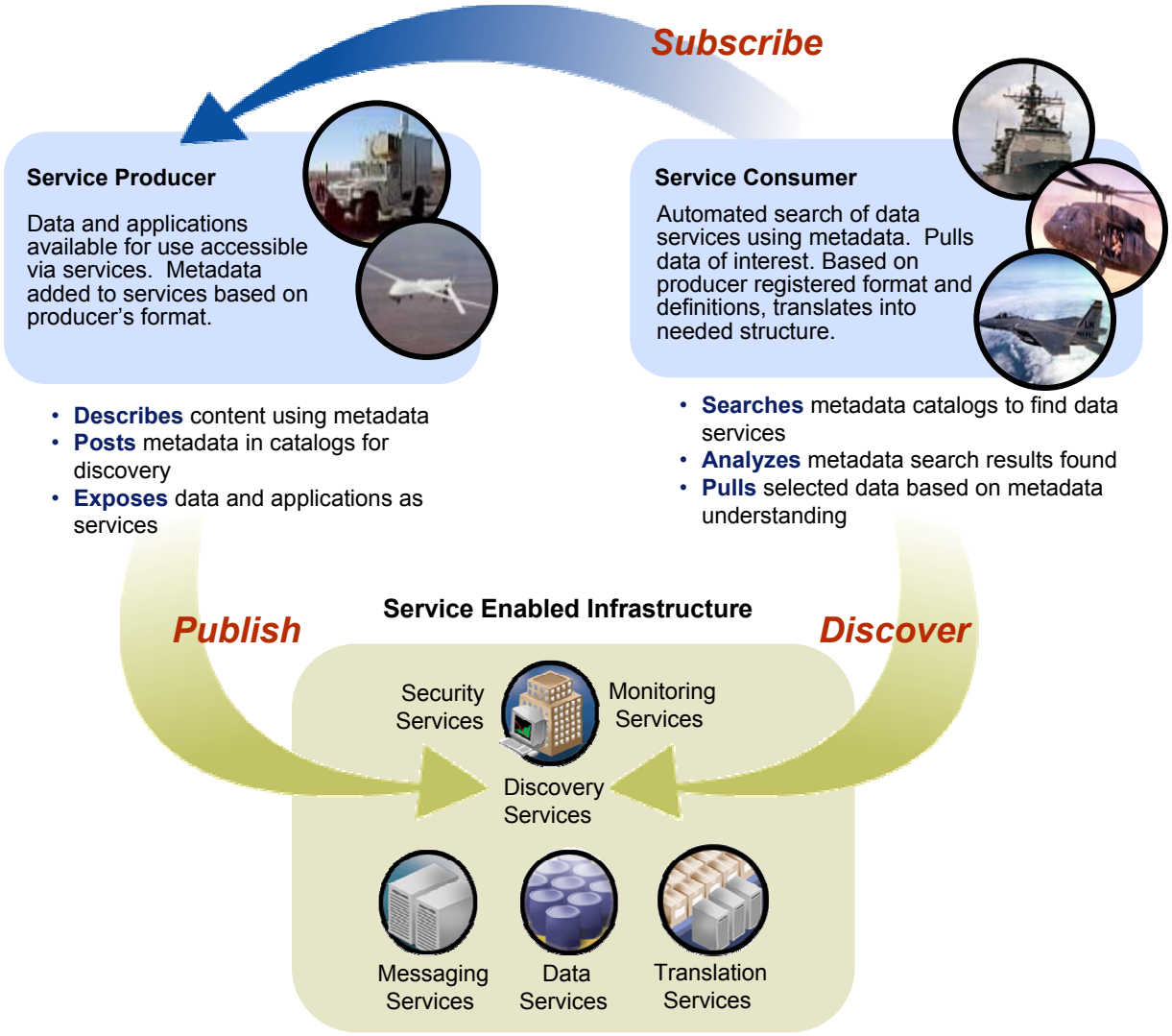


KPP	Threshold	Objective
Net Ready	Designated as Enterprise-Level or Critical to the Joint Integrated Architecture	In the Joint Integrated Architecture Values
Fusion	Automated Fusion: Level 0, Level 1 and correlate reports from all intelligence disciplines	Automated Level 3 Fusion
Reliability	90% for 72 hours	99% for 72 hours

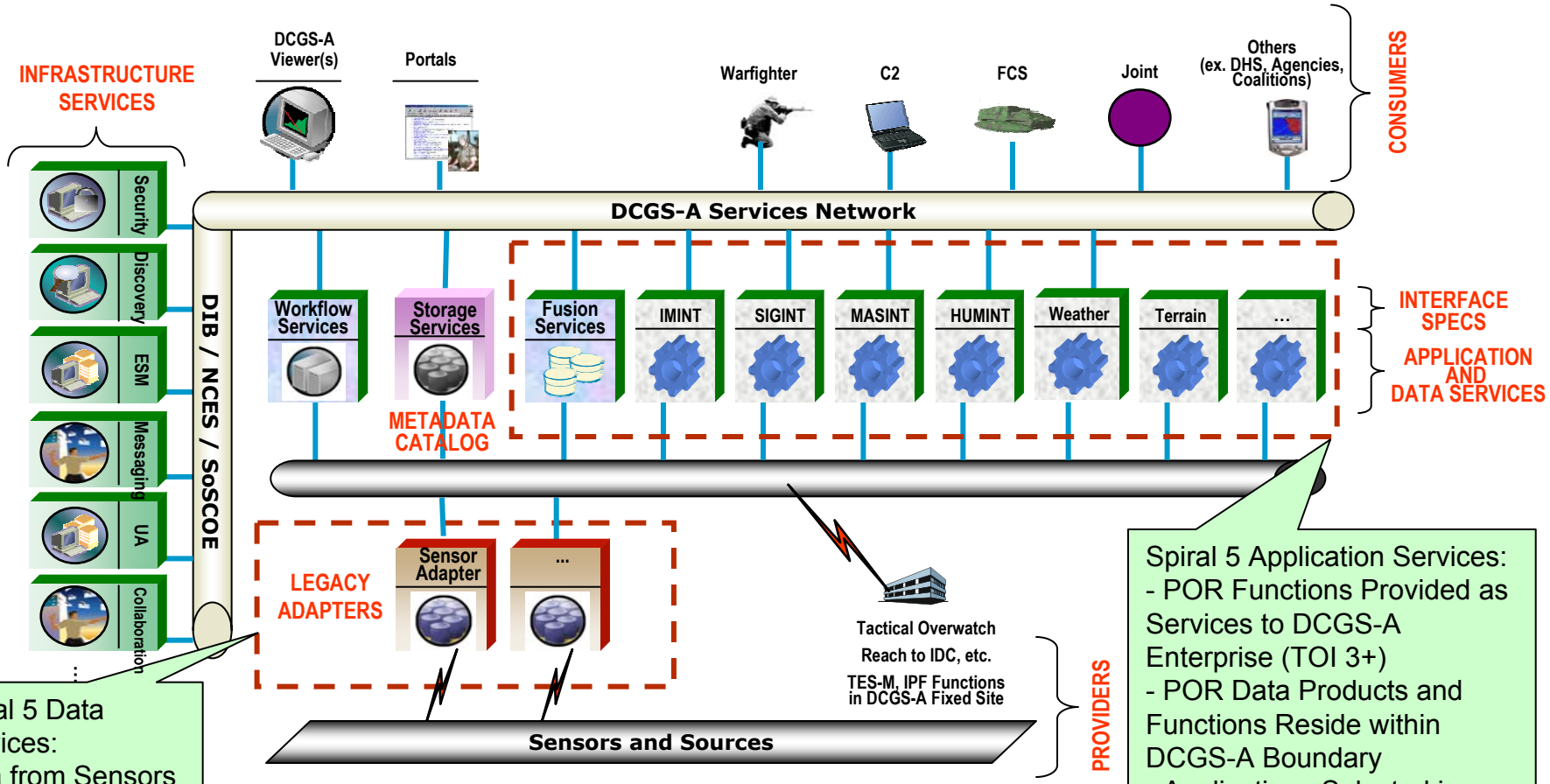
Realizing Net-Centricity - Service Oriented Architecture (SOA)

- Common perspective that Web services will do for system-to-system communications what HTTP/HTML did for the browser-based web

- Web Services are a set of XML based standards and technologies for distributed computing that characterize SOA
  - Defined in a WSDL
  - Published in UDDI registries
  - Invoked via SOAP messages



DCGS-A Spiral 5 Architecture Reference Model



Spiral 5 Data Services:
Data from Sensors and Systems at All Echelons Provided Directly to DCGS-A Enterprise

Spiral 5 Application Services:
- POR Functions Provided as Services to DCGS-A Enterprise (TOI 3+)
- POR Data Products and Functions Reside within DCGS-A Boundary
- Applications Selected in DCGS-A SIL Using Best Value Process

Case Study #4
Joint Integrative Analysis and Planning Capability (JIAPC)

An IO capability that could be applied to the home game in a non-kenetic, non-destructive way

Joint Integrative Analysis and Planning Capability (JIAPC) Description and Overview

- JIAPC is a large scale Systems Delivery effort to provide Effects Based Transformational IO Capabilities

- JIAPC will provide a collaborative environment to facilitate fully integrated nodal and network analysis for effects based operational support with standardized processes, enhanced analysis and planning capabilities, seamless target characterization, and timely response to planning requirements for lethal and non-lethal options for courses of action

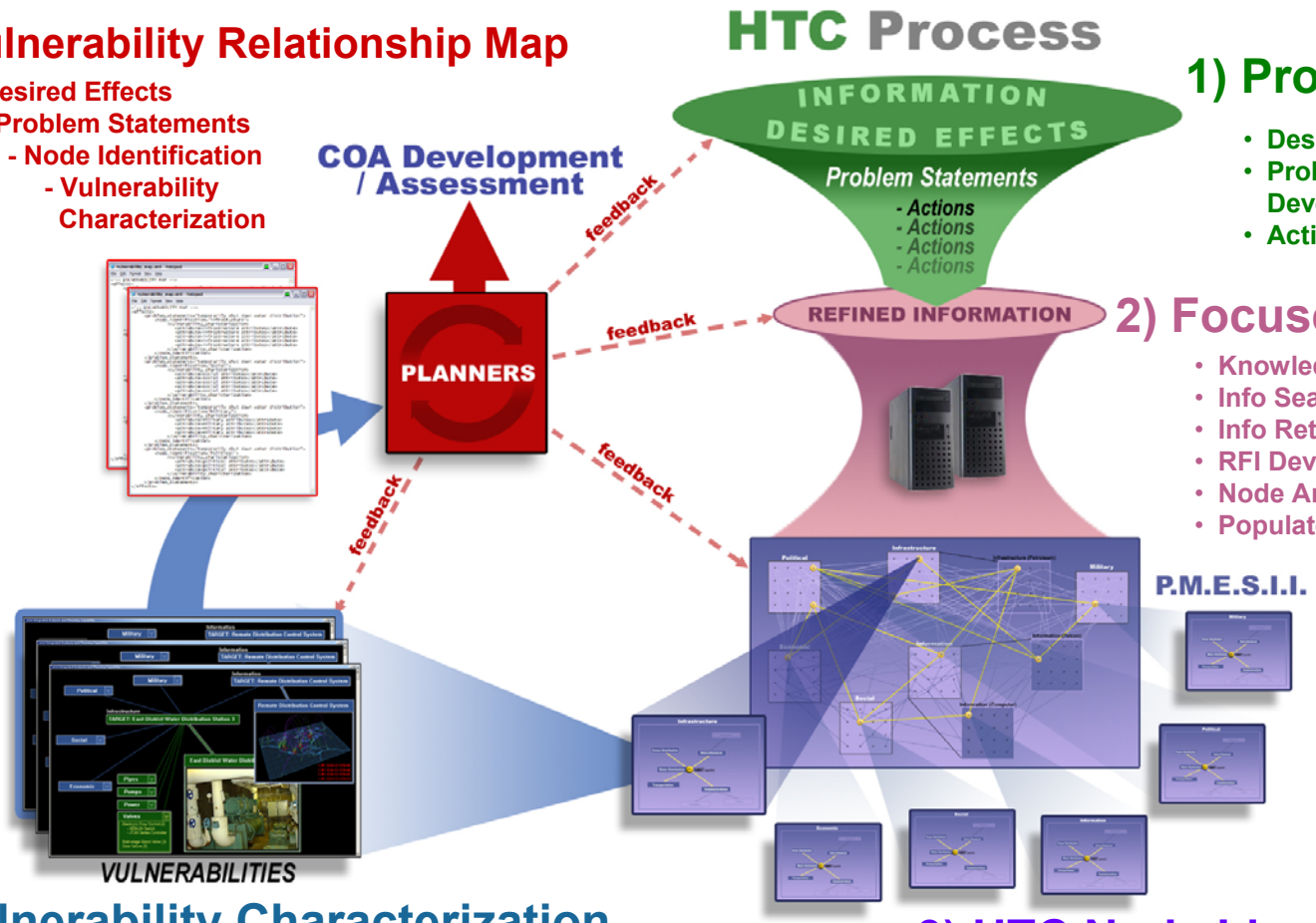
- JIAPC will provide the following capabilities:
  - Connect with Stakeholders to access Intel & other IO Information sources
  - Support "Integrative Analysis" through Knowledge Management, Visualization and Decision Aids
  - Provide the results of Integrative Analysis to the Joint IO Planning Capability (IOPC-J) in a tightly integrated and iterative manner in support of both IO Planning and IO BDA
  - Support effective collaboration across the entire process

- HLD/HLS potential application involves USD(I), STRATCOM, and DHS

Holistic Target Characterization (HTC) Process Definition

5) Vulnerability Relationship Map

- Desired Effects
  - Problem Statements
    - Node Identification
      - Vulnerability Characterization



1) Problem Definition

- Desired Effect Refinement
- Problem Statements Development & Vetting
- Action Assignments

2) Focused Data Integration

- Knowledge Discovery
- Info Search/Query
- Info Retrieval
- RFI Dev/Refinement
- Node Analysis
- Populate PMESII Templates

4) Vulnerability Characterization

- Specific Nodal System Evaluation
- Potential Vulnerability Estimates

3) HTC Node Identification

- Knowledge Discovery
- Layered Analysis
- Cross Domain Analysis
- Center of Gravity Identification
- Pattern Recognition
- Non-Obvious Node-Relationship Validation

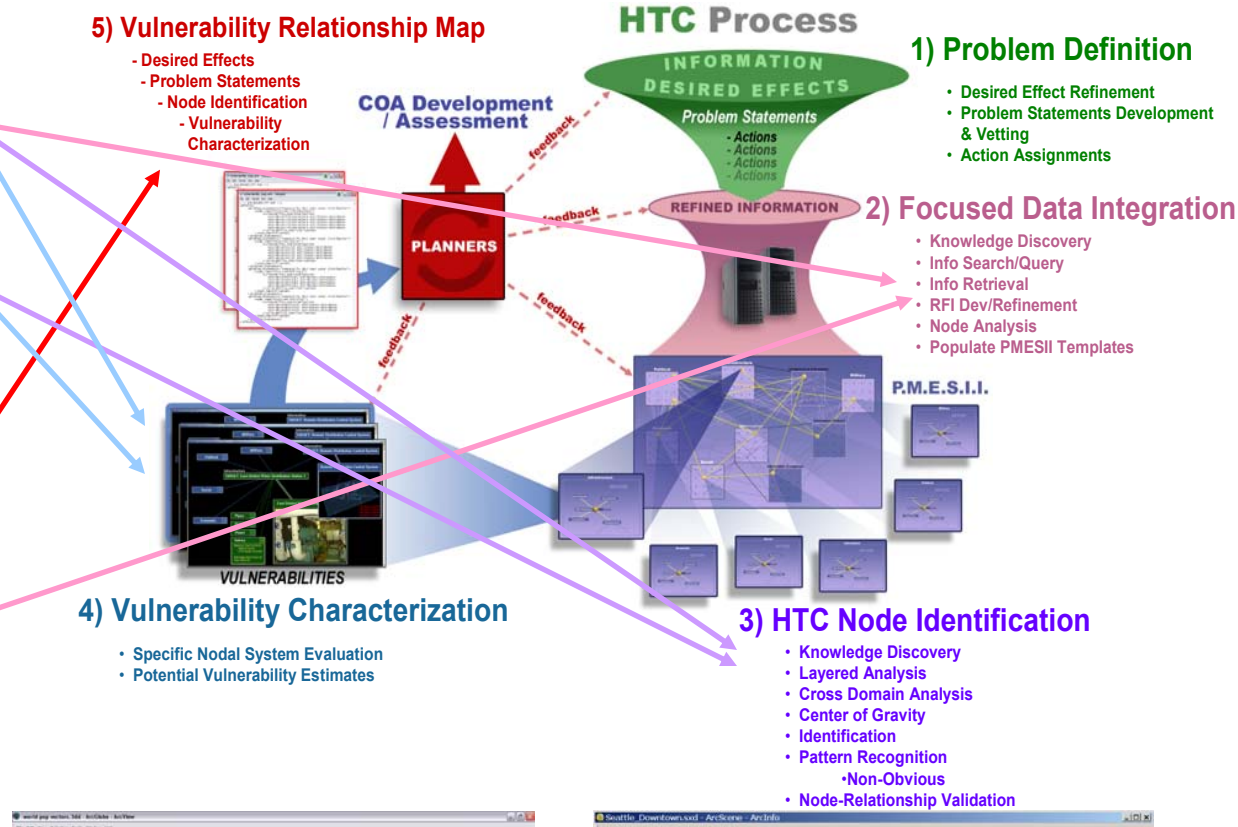
ESRI GIS Tools 1

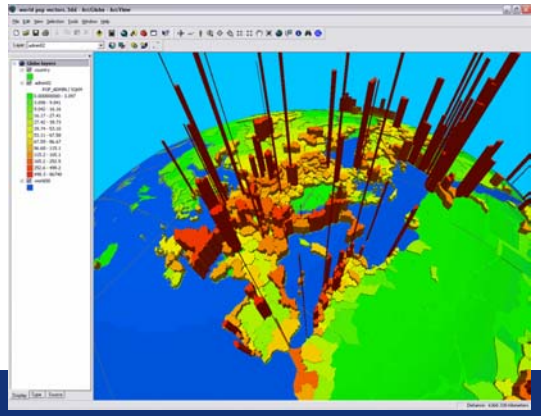
ESRI ArcGIS 9.1 is a collection of software products that enables users to analyze and visualize geographic information

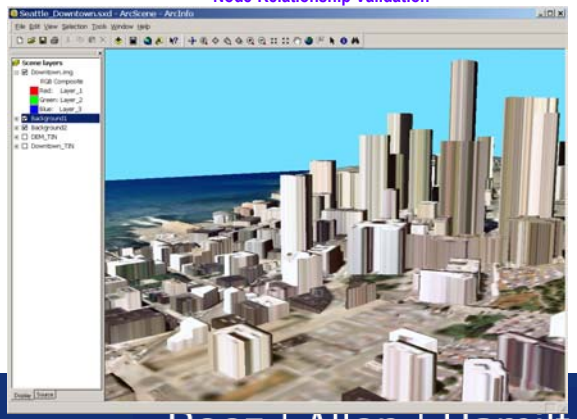
3D Analyst: Manipulate and visualize extremely large datasets in three dimensions

Publisher: Create rich interactive maps that usable without an ESRI license

Data Interoperability: Enables quick integration of various types of datasets







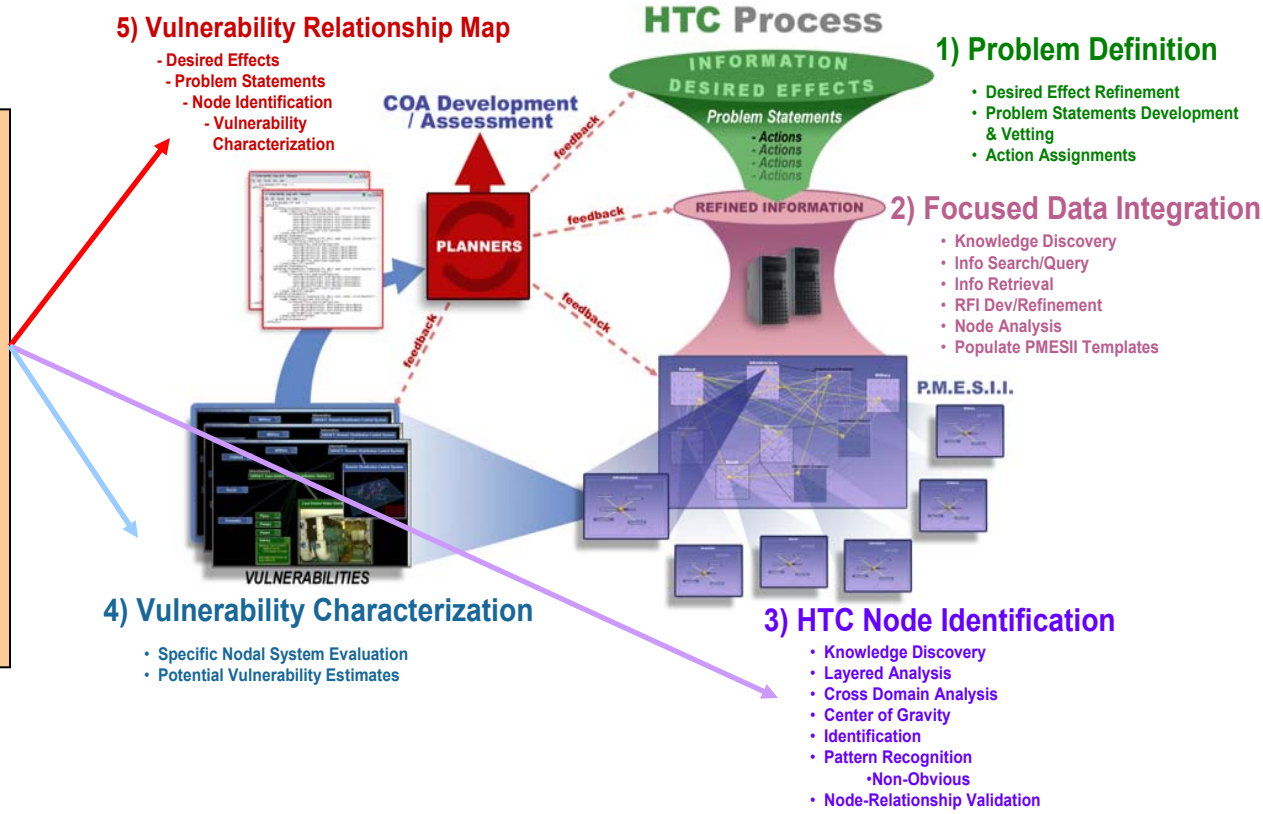
Netviz

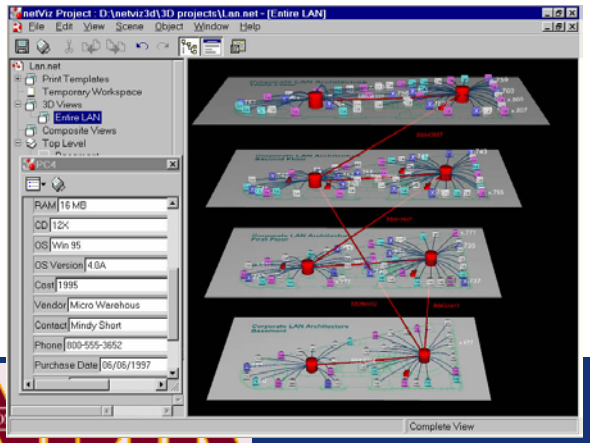
Netviz:

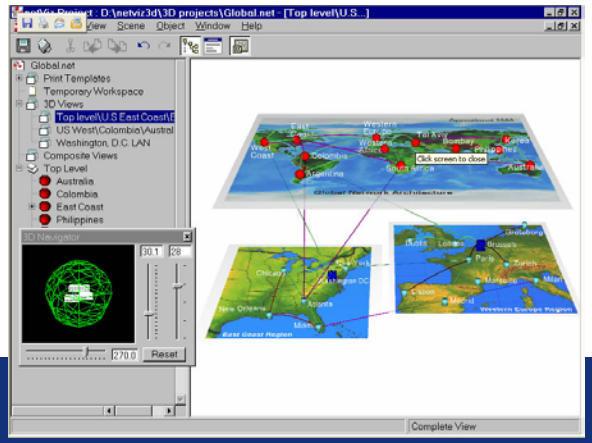
– Supports data exchanges with multiple standard interfaces (SQL, ODBC, etc.)

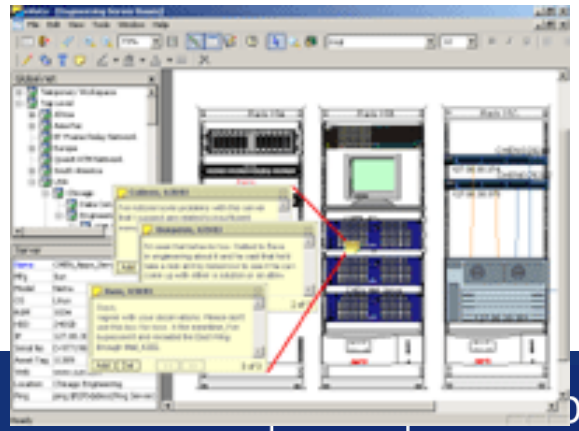
– Ability to visualize complex relationships in an intuitive manner

– Leverages existing disparate data and knowledge bases to build consolidated visual representations of their complex networks and systems









Critical Success Factors for applying proven enabling technologies to HLD/HLS missions

- Develop the **operational processes and procedures** to apply these IT technologies to the HLS/HLD environment – and then **train and rehearse**!
- Develop **policy** to mandate the use of **standards** and address the **legal issues**
  - Continue to develop interagency sharing
  - Frame the enterprise architecture
  - Address the complexities of the CONUS AOR and the impact to citizens
- Appropriately implement the **standards and specifications** to enable interoperability means that Standards will be crucial to the process
  - National Technology Transfer and Advancement Act (NTTAA) of 1995 – Public Law 104-113 (1996)
    - Requires U.S. Government organizations to explain failures to use commercial standards when such standards meet their needs
    - Requires U.S. Government organizations to adopt commercial standards wherever possible – particularly those that standards developing organizations have developed – in lieu of creating proprietary, non-consensus standards

Questions and Answers

Booz Allen Contact Information

Angela Messer
Principal

Booz | Allen | Hamilton

Booz Allen & Hamilton Inc.
8283 Greensboro Drive
Mclean, VA 22102
(703) 902-5666
Messer_Angela@bah.com