Space Ground Services in the Joint Information Environment (JIE)

Scott Niebuhr, Jeremy Burton, Judy Kerner, Sky Troyer
The Aerospace Corporation

© 2015 The Aerospace Corporation

Space Ground Services in the Joint Information Environment

Agenda

- What is the JIE?
- JIE Operational Evolution
- Approach to Achieving the Anticipated Outcomes
- Current Implementation Status
- How Will Space Ground Systems Leverage JIE?
- Potential JIE Ground Systems Impacts and Benefits
- Evolving Ground System Acquisitions
- Next Steps for Ground System Developers

What is the JIE?

The Joint Information Environment (JIE) is a secure and flexible data-centric information environment based on commercial information technology (IT)

- *Shared network infrastructure*
- *Common enterprise services*
- *Single security architecture*

– *Its objectives are to:*

- *improve mission effectiveness*
- *decrease cyber attack surface*
- *realize IT efficiencies*

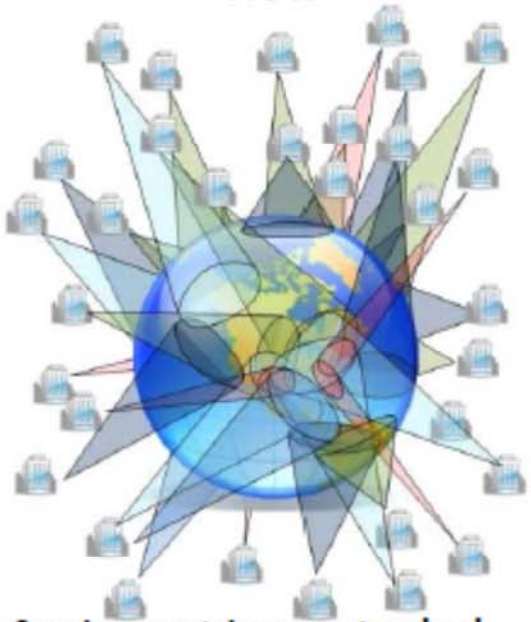
JIE is operated and managed per the Unified Command Plan (UCP)

- *using enforceable standards, specifications, and common tactics, techniques, and procedures (TTPs)*

Adapted from Charter for The Joint Information Environment Management Construct, 4-Star JCS TANK approved definition 6 August 2012.

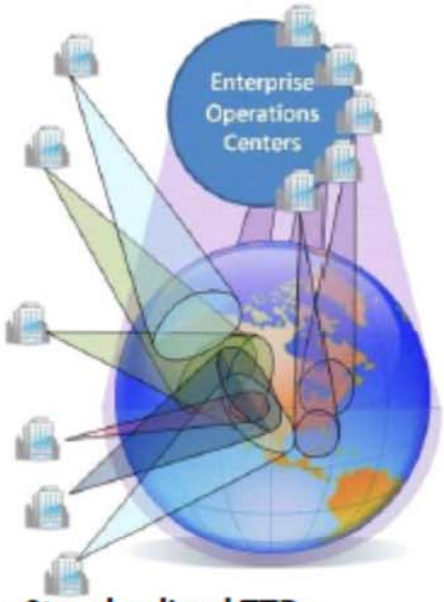
JIE Operational Evolution

Now



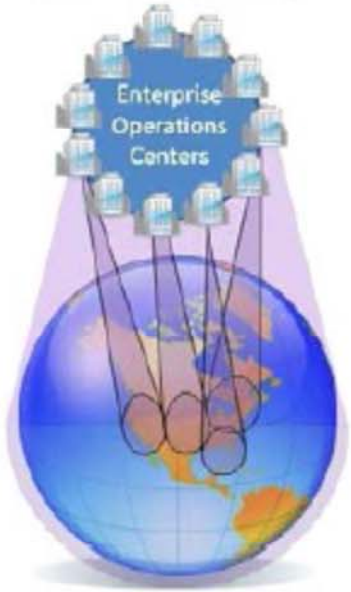
- Service-centric non-standard operations centers
- Non-standard TTPs, architectures & applications
- No standard ops architecture

JIE Interim



- Standardized TTPs
- JIE ops architecture
- GEOC established
- Initial JIE COP capability
- Mixture of JIE EOCs and Service operations centers
- Reduced number of CNDSPs

JIE End State



- Fully meshed EOCs provide seamless control and failover
- GEOC at full operational capability
- EOCs in place for all non -Service unique missions
- JIE COP in place
- Automated capabilities in place, e.g. compliance verification and reporting

EOC – Enterprise Operations Center
CNDSP – Computer Network Defense Service Provider
GEOC – Global Enterprise Ops Center
COP – Common Operational Picture

Figure reprinted courtesy of DoD

Approach to Achieving the Anticipated Outcomes

- Single Security Architecture (SSA)
- Network Normalization
- Identity and Access Management (IdAM)
- Enterprise Services
- Data Center Consolidation
- Cloud Computing

Adapted from the DoD Strategy for Implementing JIE

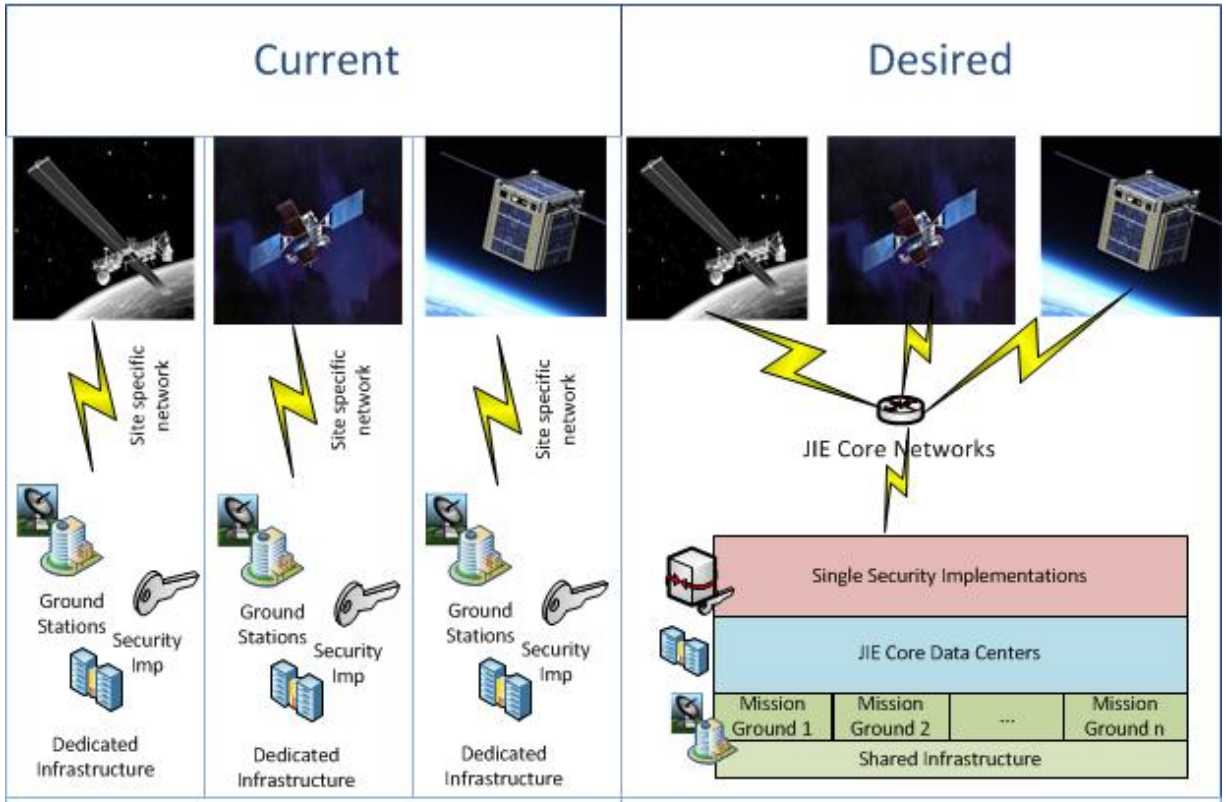
Current Implementation Status

- Common infrastructure and services, combat support applications
- EUCOM implemented first – Networks, Operations Centers, JRSS
- JRSS implementation in CONUS
  - *Joint Regional Security Stacks (JRSS) first in place in Joint Base San Antonio (JBSA)*
  - *JRSS are beginning to be operational in CONUS*
  - *Monitoring and testing effectiveness, impacts*
- Implementing services
  - *Software Application Rationalization and Server Virtualization*
  - *Desktop Virtualization and Thin-Client Environments*
  - *Mobility Services*

Figure reprinted courtesy of DoD

How Will Space Ground Systems Leverage JIE?

Notional Evolution of Infrastructure



Characteristics:
- Custom/Site Unique monitoring and troubleshooting
- Site specific, dedicated network
- Custom security implementation
- Dedicated HW including servers, storage, network equipment, monitoring and security equipment

Results:
- Duplicated infrastructure
- Site specifics, adding new system would mean adding new network , security implementations
- Increased C&A efforts when adding new systems

Characteristics:
- Utilizing JIE Core Network and DISA teleport
- Utilizing JIE Single Security Implementation
- Utilizing JIE Core Data Centers, shared infrastructure i.e. common compute, storage etc
- (Future) Common Ground Architecture

Results:
- Software Defined Network means reduced duplication for network, site equipment and security implementations
- Scalability and adaptability when acquiring new systems
- Reduced implementation, maintenance and C&A efforts

Figure by Sky Troyer, The Aerospace Corporation.

Potential JIE Ground Systems Impacts and Benefits

- Common Infrastructure / Services
  - *Developers can focus less on IT, more on the mission*
  - *Agile development environment, allows quick transition to operations*
  - *Use of Software Defined Networking*
  - *Improve sustainability, scalability, maintainability*
  - *Reduce procurement time and cost*
- Joint Regional Security Stacks
  - *Automated security monitoring, Defensive Cyberspace Operations*
  - *Reduce time and effort spent on Assessment and Authorization (formerly known as Certification & Accreditation)*
  - *Improve vulnerability management, reduce time spent on patch management*
  - *Reduce required staffing, training costs*
- Common data access
  - *Shared data can be located on a common platform and common namespace*
  - *Scalability, security concerns can be addressed jointly*
  - *Help with load balancing, redundancy, resource availability*
- Joint Governance
  - *Every application and system must meet the same rules and standards*

Joint Regional Security Stack

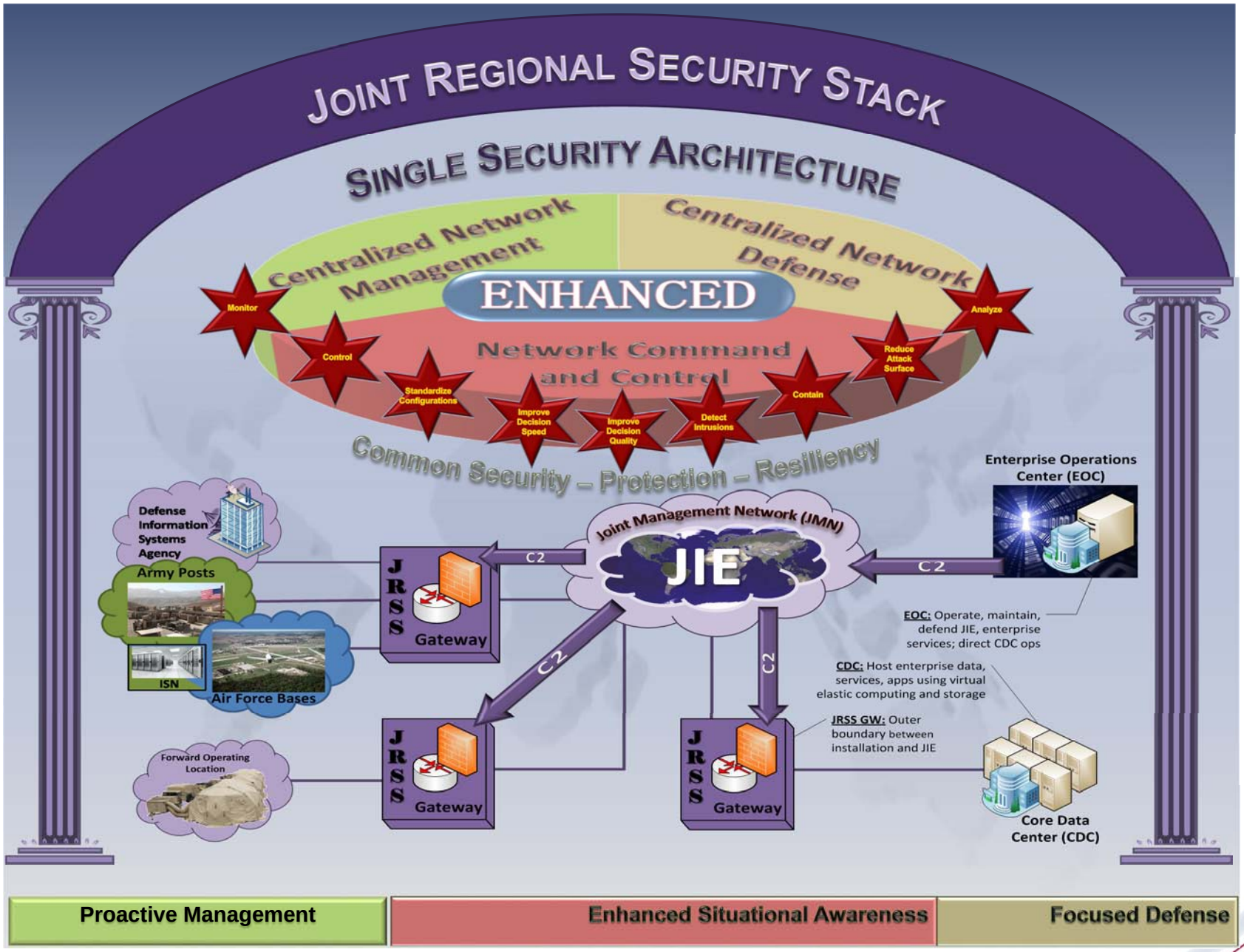


Figure reprinted courtesy of DoD

Joint Regional Security Stacks

- "As a key component of the Joint Information Environment's (JIE), the Joint Regional Security Stack (JRSS) will consolidate network transport and security boundaries across the DoD. JRSS brings a Single Security Architecture (SSA) to JIE by providing enhanced:
  - *Centralized Network Management; the ability to manage the network proactively; controlling, monitoring, and analyzing network activity and events*
  - *Centralized Network Defense; offering focused defensive capabilities; detecting, analyzing, and containing intrusions*
  - *Network Command and Control; providing enhanced situational awareness (SA); improving the speed and quality of command decisions*

- The JRSS will connect AF and Army network resources at permanent installations and in forward operating locations to the JIE via gateways managed under DISA oversight... Installation Service Nodes will provide network services for an individual installation to operate in a disconnected state. The gateways will provide managed and protected connection to Core Data Centers (CDC), providing warfighters and their support organizations secure access to services and information."

From JRSS Architecture Development Update, Air Force Network Integration Center, AFNIC / NAS, Mr. Steve Stoner, 15 Jul 2014.

Evolving Ground System Acquisitions

- Identify unique information technology needs
  - *Define performance requirements*
  - *Define criticality of components and mission threads*

- Consider JIE services first
  - *Cloud Computing Services: Application Licensing, virtualization*
  - *Consolidated Data Centers: Configuration and Data Management*
  - *Collaboration Services: DCO/Unified Capabilities*
  - *Defensive Cyber Operations: Joint Regional Security Stacks (JRSS)*
  - *Leverage common infrastructure, focus on truly mission-unique requirements*

Ground Services Will Be an Integral Part of Consolidated Enterprise Services

Next Steps for Ground System Developers

- What GS developers should do now
  - *Keep current on JIE, engage JIE POCs*
  - *Architect systems to take advantage of common resources (JRSS, enterprise services, consolidated data centers, etc.)*
  - *Provide ground system requirements to JIE use cases/scenarios and enterprise services*
  - *Volunteer to be pathfinders to ensure the JIE meets programs' needs*
  - *Share information from prototypes, pathfinders, and pilots*
- SMC/ENP is working with AFSPC, AFLCMC, and SAF/CTO on:
  - *Space-focused and JIE-integrated Enterprise Security Architecture*
  - *Guides and plans to leverage Joint Regional Security Stacks*
  - *Prototypes and SMC-wide implementation plan for JIE services*
  - *JIE-integrated Enterprise Knowledge Management System*
- Programs should establish communications with POCs on JIE
  - *SMC programs should work with SMC/ENPM*

Space Ground Systems Can Be at the Forefront of the Transition to JIE

QUESTIONS?

Backup Slides

JIE OV-1

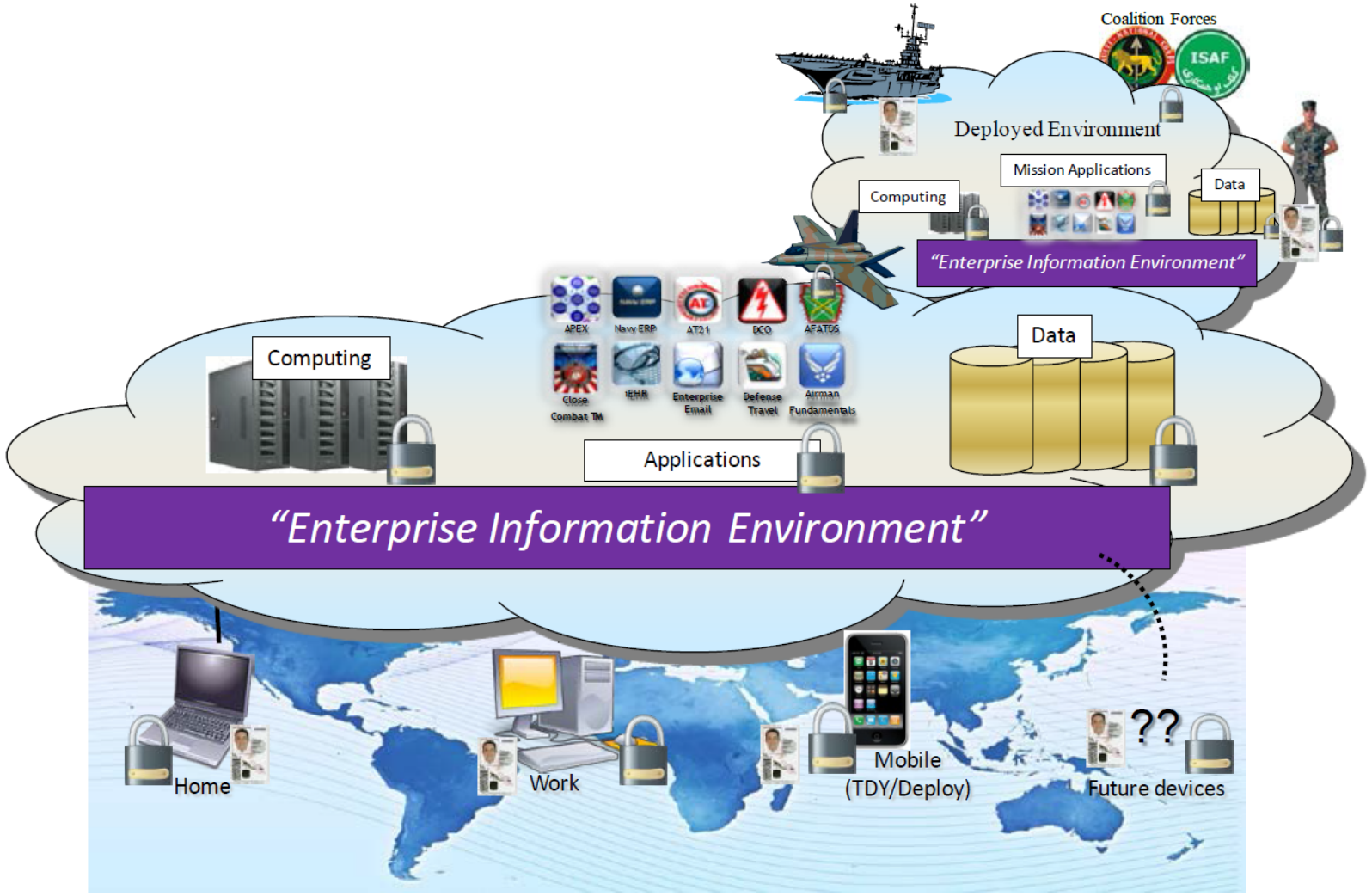


Figure reprinted courtesy of DoD