



Architecting for Resiliency

Army's Common Operating Environment (COE)

SERC

5 October 2011

Mr. Terry Edwards

Director, ASA(ALT) Office of the Chief Systems Engineer (OCSE)

(703) 614-4540

terry.edwards@us.army.mil





Operating Environment

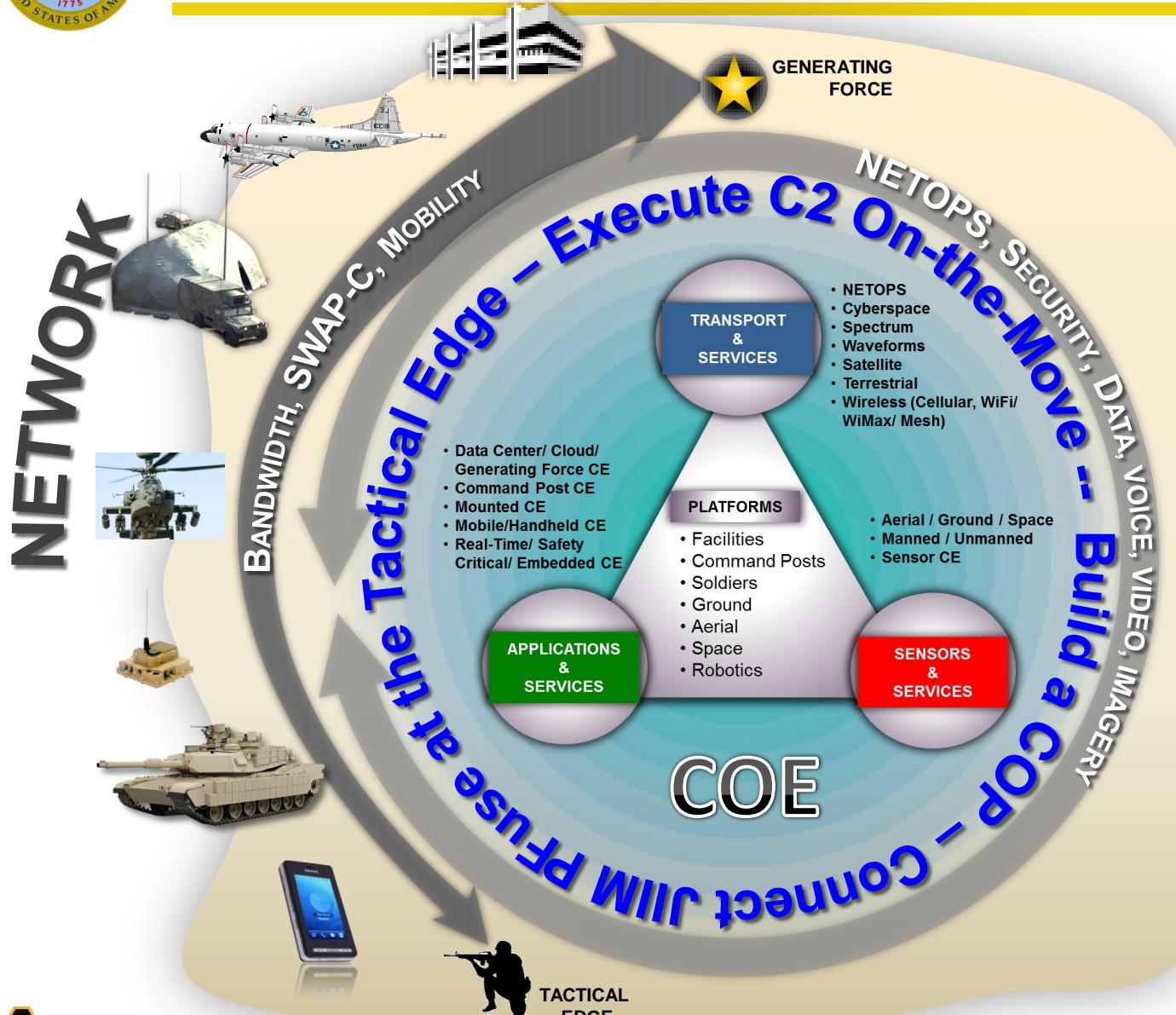


- Uncertain futures & threats outpace our ability to create & field affordable, effective systems
 - Change happens – we need to design for it
 - Adaptability, trustability and affordability must be considered
 - Need to have agility in dealing with requirements change
 - Long design times – exacerbate uncertain future problems, overload designs, and lock out new technologies





Common Operating Environment For the NETWORK



*COE is an approved set of **computing technologies and standards** that enable secure and interoperable applications to be rapidly developed and executed across a variety of Computing Environments*

*Source: Army CIO/G6
COE App C*





COE Implementation Goals



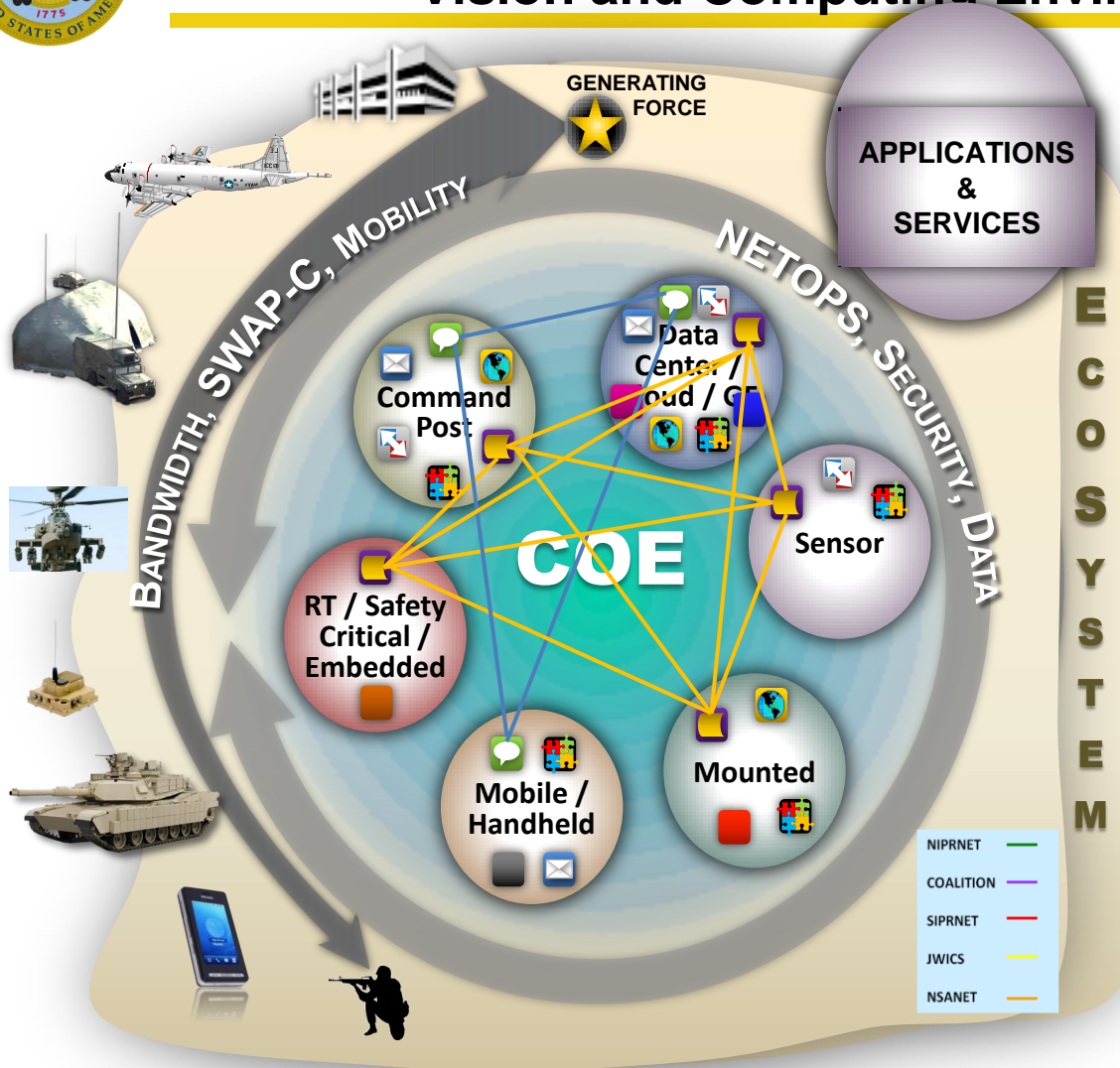
- Standards-based / Industry-driven solutions IAW the CIO/G6 Technical Architecture
- Single Foundation within a Computing Environment (CE)
 - Strategic approach to software re-use
- Abstract software applications from HW/SW infrastructure
 - Reduce lifecycle cost improve supportability
- Foster an agile environment that enables 3rd party development
 - Direct user involvement in Apps development
- Reduce testing and certification timelines
 - Improve speed to market
- Leverage government labs/support structures to fullest extent

Promote innovation and aggressively pursue efficiencies





Apps & Services COE Building Blocks: Vision and Computing Environments



Organize Computing Environments

- Scope of COE implementation requires systematic and manageable approach
- Clustering similar systems based on mission environments to facilitate implementation

Resilient Architecture Design is essential to our Business





Resilient Design



- Build redundancy, flexibility and adaptability into the architecture
 - Leverage Cloud concepts and capabilities
 - Open architectures
- Build robust foundations that is Cyber hardened and resilient
- Leverage process and technology to take on trustability
 - Attribute based identity management
- Built in smart technologies to continuously gauge the health and state of the network.
- Using real live data to model the deployed network to conduct what-if drills.
- Method to dynamically quarantine, isolate and update capability in a deployed state





Establishing the Environment for Resilient Design



- Establish the environment to conduct design trades and product evaluations
 - C4ISR Center of Excellence – Aberdeen Proving Ground, Maryland
- Methodology to evaluate product designs - especially for COTS products
- Architecture through modeling and simulation
- Benchmark testing of critical components
 - Component Labs across the ARMY R&D community
- Instrumented virtual and live environments
 - Ft. Bliss, TX - Agile Testing & Evaluation environment





Acquisition Objectives – for the COE



The Army's COE Implementation Strategy is ..

not only addressing fixing interoperability within the Force, but also accounts for critical strategic level goals as well

- Achieve agility on how we deliver capabilities to the Warfighter faster *(Vice Chief of Staff, 14 Apr 2011)*
- Reduce the life cycle cost of development and sustainment of our IT systems *(DoD Efficiency Initiatives, 16 Aug 2010)*
- Promote an Open Architecture that is standards based which leverages industries best practices and products while reserving government purpose rights *(Implementation Directive for Better Buying Power, 3 Nov 2010)*
- Build on a foundation that is cyber hardened and secure *(Cyber Command)*

