Net-Centric Systems Design and Requirements Development in today's environment of Cyber warfare

2015 NDIA Systems Engineering Conference
Dr. Craig Arndt
Defense Acquisition University

Agenda

- Requirements
- Background
- Trends
- Issues and problems
- Systems Engineering approach
- De-conflicting requirements
- Test and Evaluation
- Integration
- Conclusions and recommendations

Requirements

- Interoperability
  - Visibility
  - Command and control
  - Data transfer
- Security
  - Authentication / authorization
  - Traffic monitoring
  - Incretion detection

Net-Ready Key Performance Parameter (KPP)

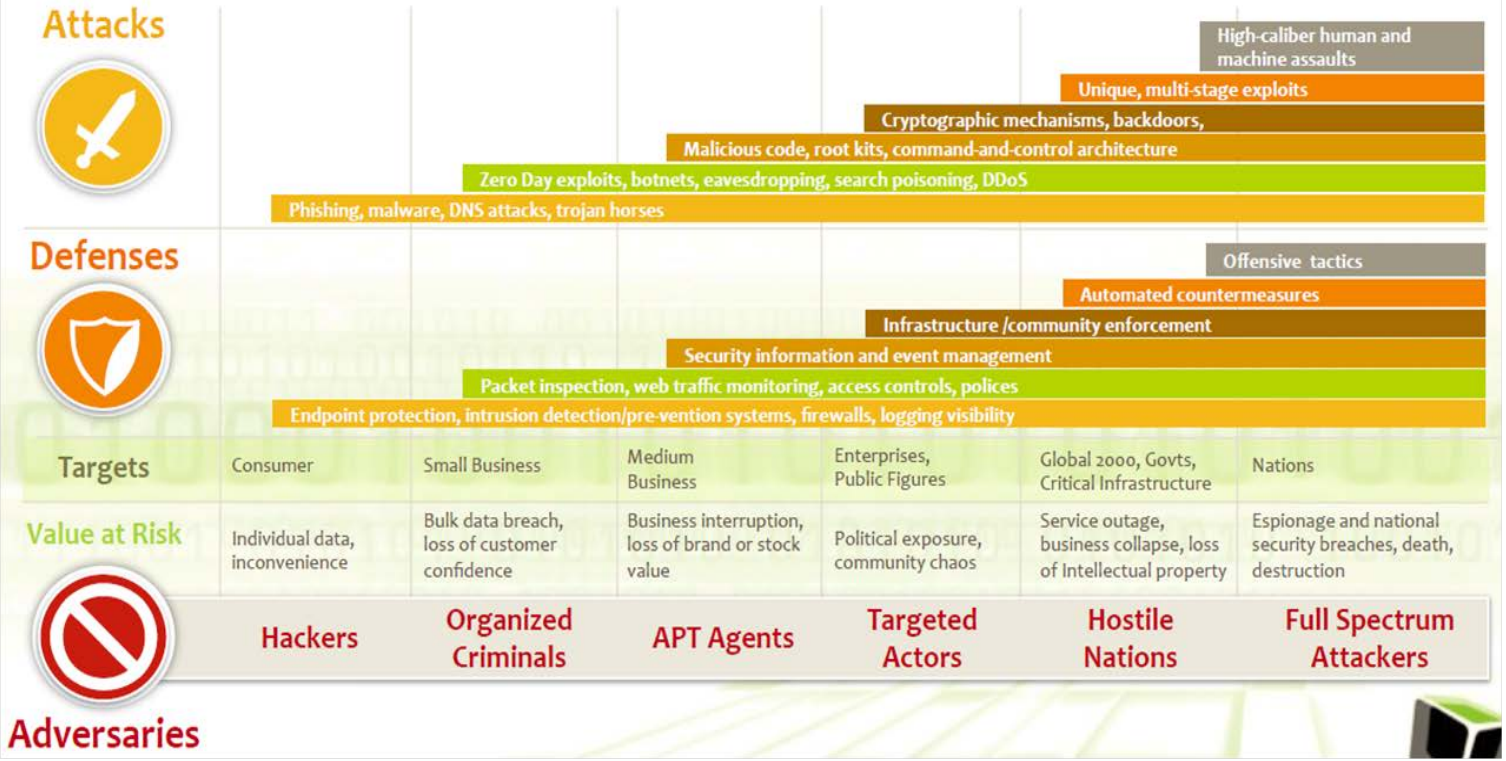
Net-ready attributes determine specific criteria for interoperability, and operationally effective end-to-end information exchanges which are traceable to their associated operational context, and are measurable, testable, and support efficient and effective T&E.

Background

- Interoperability
  - Interoperability increases effectiveness
  - Reduces cycle time
  - Is a force multiplier
- Threats
  - PII
  - Denial of Service
  - Hidden malware

Threats

Defense Science Board/KEYW Cyber Threat Taxonomy: The Spectrum of Attacks and Defenses

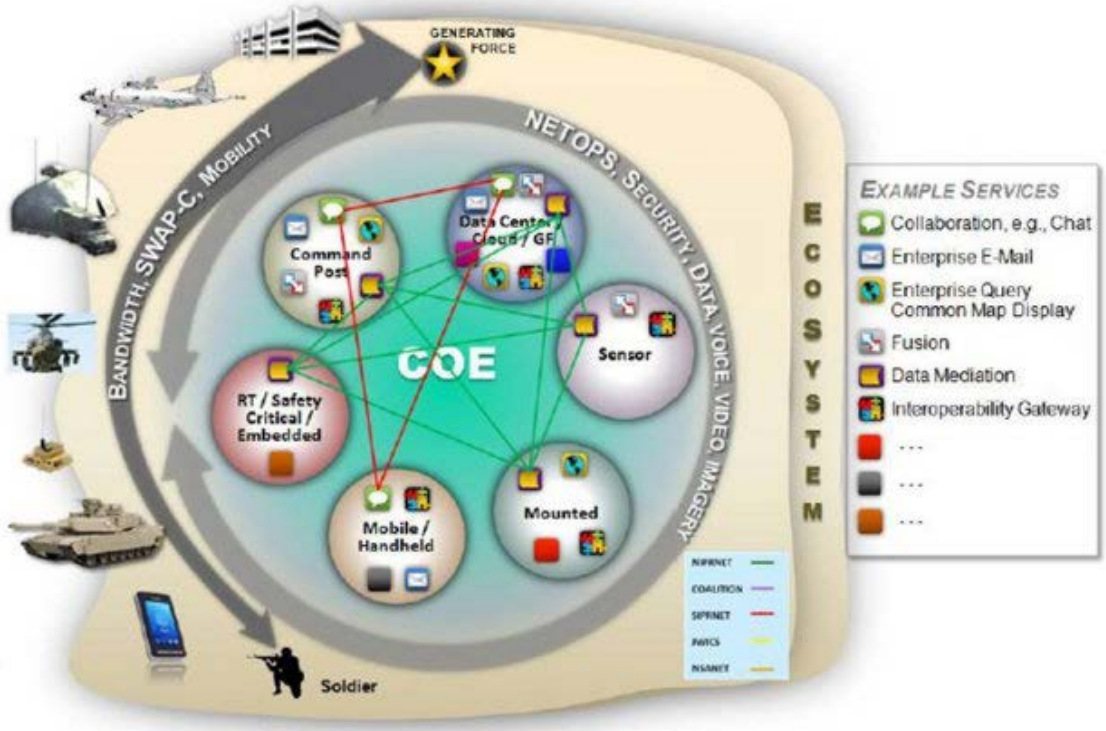


Trends

- Dependency on COTS and commercial systems and Networks
- Attacks though connected networks
- Insider Threats
- Cloud Data Storage
- Embedded sensors

Army Releases Common Operating Environment Implementation Plan

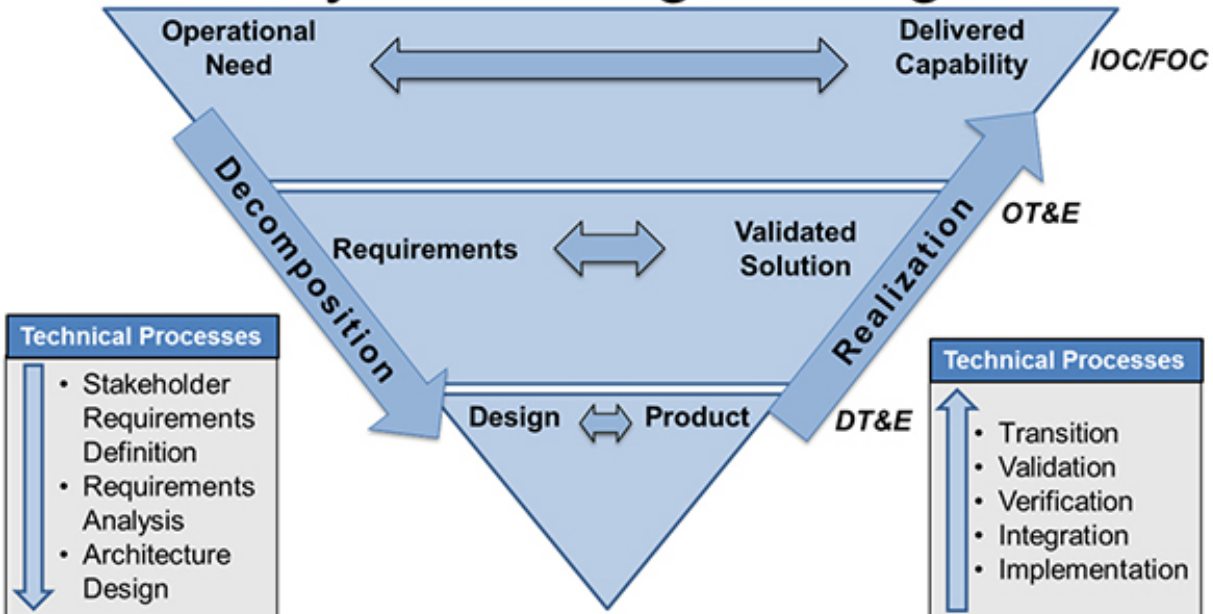
The U.S. Army has formally unveiled its Common Operating Environment (COE) Implementation Plan, an effort consisting of an Army's plan to modernize equipment and weapons systems around a common set of IT standards and architecture as it develops a truly networked force. (January 10, 2012)



Issues and problems

- Remote conductivity needed for interoperability and net-centric operations also can increases vulnerability
- The cost of dedicated networks can be prohibitive
- The use of commensal networks, hardware and software decreases cost and reduces development time

Systems Engineering

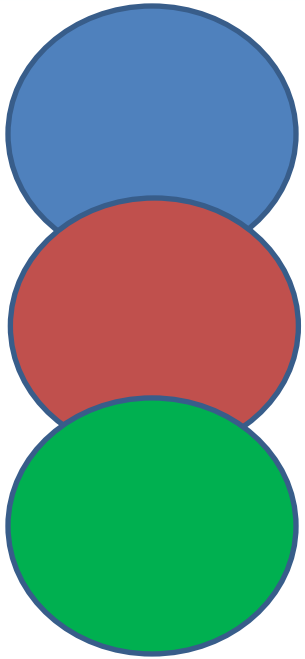


De-Conflicting

- Requirements analysis requires de-conflicting of the requirements for security and improved performance.
- In addition to interoperability and net-centricity we also have the requirements of reduced cycle time, reduced cost, and increased use of COTS
- If we optimize these requirements independently we will continue to have significant vulnerabilities for advisories to exploit
- Optimizing these requirements together will require significantly greater requirements, development and operational corporation between the different key organizations
  - Venders
  - Government
  - Researchs

Cyber Security

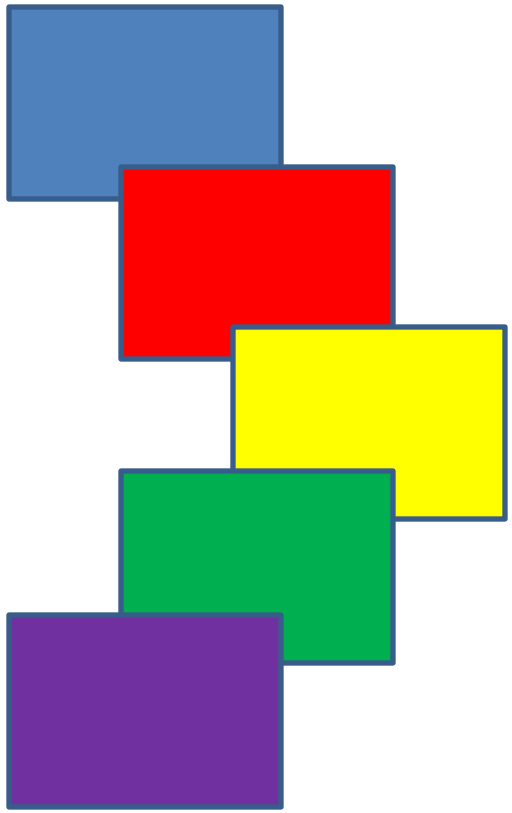
- Response
- Denial
- Resilience



DoD Cyber Strategy, April 2015

Interoperability

- End-to-end information exchanges
- Command and Control
- Multiple levels and locations of processing
- Data Aggregation and Fusion
- Data to information to knowledge to decisions



Test and Evaluation

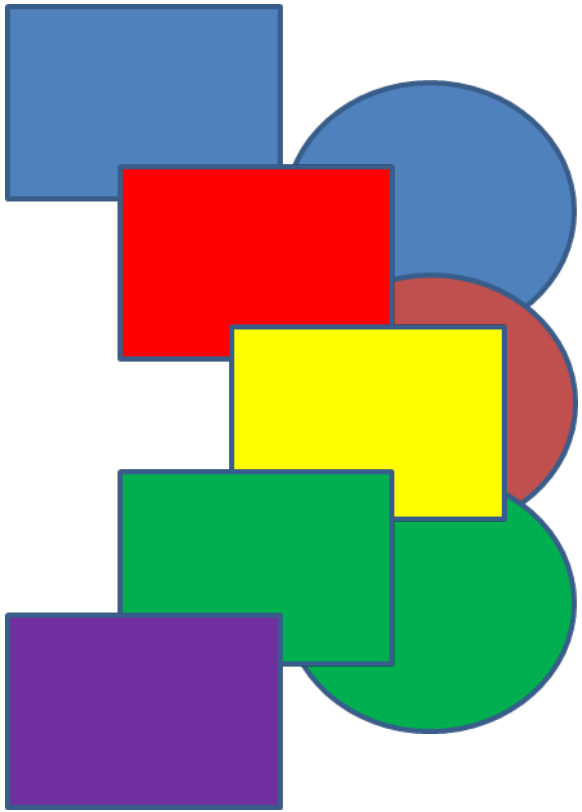
- Testing and evaluation plays a critical role in the development of systems suitable for the critical operational environments
- Past testing protocols are not adequate for new interconnected COTS integrated networks
- Continues testing is now required for all classes of systems and system interfaces
- New levels and methods for testing can serve as triggers for offensive and defensive actions in the future

Integration

- The integration of networks and systems add significant utility / capability and significant risk to all classes of systems
- Current and future generations of integrated systems need to be able to de-integrate and conduct operations in mutable non-integrated and semi-integrated modes
- There is a need to develop
  - Alternate
    - Software
    - Configurations
    - Modes of operation

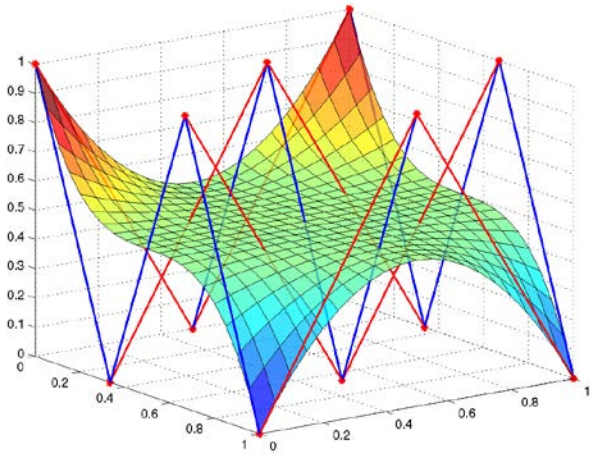
What the Solutions Mite Look Like

- Elimination of critical vulnerabilities (passwords, insiders, authentication, etc.)
- Commensal developers working more closely with government, users, and researchers
- Better testing and monitoring systems
- Continuously reconfiguring networks
- Systems and networks capable of de-integrating and operating independently in normal and emergence operations



Multivariate optimization problem

- Key research problem for the future
- Will require characterizing the goals of
  - Security
  - Interoperability
  - Cost
  - Speed
  - Reliability



Conclusions and Recommendations

- Research
  - Use advanced analysis methods for determining optimum requirements configurations
- Robust testing
  - Initial and ongoing, testing, with embedded triggers
- Increased use of dynamic de-integration of systems
  - Continuously on Radom time intervals and configurations
- New ways to use COTS products
  - Additional software
  - Multiple operating environments
- Increase the collaboration of different developers, and operators to develop better optimized solutions to security and interoperability needs