Advanced Persistent Threat: Requirements Challenges

ITEA 2nd Cyber Security Workshop: Test and Evaluation to Meet the Advanced Persistent Threat

Matt Maier, Director, ASA(ALT) Cyber Focal, System of Systems Engineering and Integration (SOSE&I)

DESIGN / DEVELOP / DELIVER / DOMINATE

25 February 2015

The Cyber Environment

DESIGN / DEVELOP / DELIVER / DOMINATE

- The Threat…
  - is constantly changing and evolving
  - is becoming increasingly sophisticated and dangerous

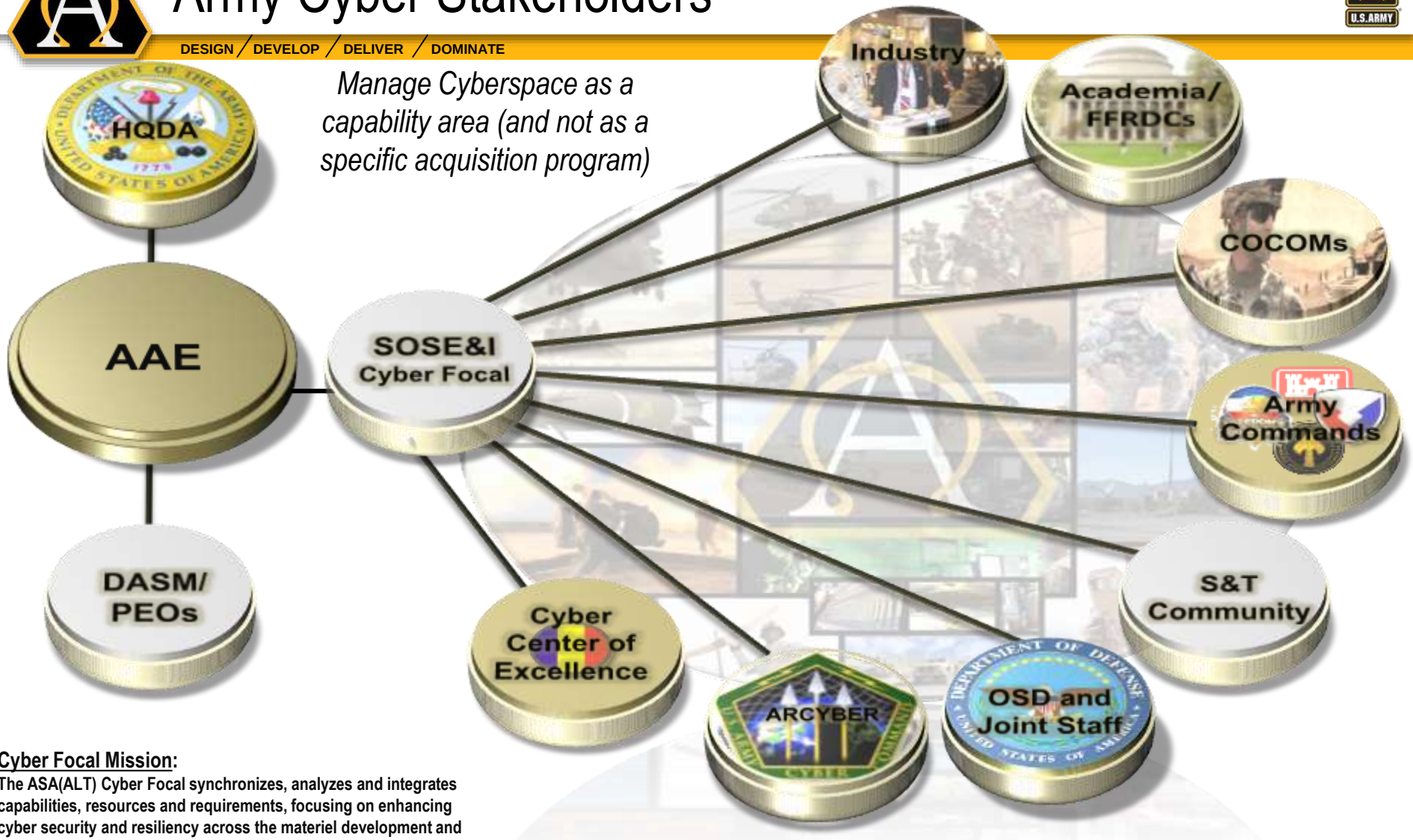
- Cyberspace technology spans…
  - Enterprise and tactical networks
  - Joint and coalition networks
  - National and international boundaries
  - Federal, commercial, academic and private sector networks
  - Wired, fiber and electromagnetic spectrum

- Army Approach
  - Given the pace of technology, Army must be innovative and responsive to defend and counter cyber threats
  - Cyber requires a unified approach:
    - Protect and defend the network and vital information
    - Design for cybersecurity and mission assurance/ resilience
    - Provide soldiers the ability to detect, deter and defend the network

Army Cyber Stakeholders

DESIGN / DEVELOP / DELIVER / DOMINATE

Manage Cyberspace as a capability area (and not as a specific acquisition program)



Cyber Focal Mission:
The ASA(ALT) Cyber Focal synchronizes, analyzes and integrates capabilities, resources and requirements, focusing on enhancing cyber security and resiliency across the materiel development and cyber operational communities.

Vision:
Enabling decisive cyber operations through agile materiel development.

AAE = Army Acquisition Executive
ARCYBER = Army Cyber Command
ASA(ALT) = Assistant Secretary of the Army (Acquisition, Logistics and Technology)
COCOM = Combatant Commander
DASM = Defense Acquisition System Manager
FFRDC = Federally Funded Research and Development Centers
HQDA = Headquarters, Department of the Army
OSD = Office of the Secretary of Defense
PEO = Program Executive Office
S&T = Science and Technology

ASA(ALT) Cyber Focal

DESIGN / DEVELOP / DELIVER / DOMINATE

Cyber Programs

Coordinate Cyber Capabilities Development for the Warfighter

Mission Assurance/ Resilience

Ensure Cyber Defensible/ Resilient Systems in the Army

CIO Governance

Domain Management of Defense Business Systems

Cybersecurity

Accredit, Validate and Oversee Army Systems Cybersecurity

Defense Industrial Base

Enhance and Supplement DIB Capabilities to Safeguard Information

Cyber Architecture – "Cybersecurity" engineering support to SoSE&I

Synchronize, Analyze, Integrate

Army Priorities

DESIGN / DEVELOP / DELIVER / DOMINATE

- Equipping the Cyber Force

  Responsibility for fielding Warfighting capabilities in response to Army cyberspace requirements

  - Responsive to specific, detailed Cyber Mission Force requirements
  - Defensive, Offensive, DoD Network Operations Capabilities

- Improved Network Defense

  Responsibility for ensuring fielded Army capabilities have continued mission assurance/ resilience

  - Increased authentication
  - Protected network transport
  - Improved data communication security
  - Robust tactical infrastructure

Closing Comments

- Challenges
  - Requirements, resourcing, and acquisition processes must work together to:
    - Field cyberspace capabilities to Cyber Mission Forces
    - Provide Mission Assurance/ Resilience against Advanced Persistent Threat
  - Test and Evaluation must be rapid, comprehensive and continuous
  - Lack of requirements can create challenges for acquisition and resourcing

- Way Ahead
  - Army cyberspace community should establish:
    - Rapid acquisition capability fielding process
    - Cyberspace governance structure
  - Army needs rapid, flexible risk based approach to information assurance and vulnerability management