CSIAC Workshop on M&S Support for Cyber Mission Forces

Dr. Steven E. King

Cyber Technologies Director

Information Systems & Cyber Technologies (IS&CT)

OASD(R&E)

6/27/2016

Historical Need for Cyber M&S

- **2011 Cyber Priority Steering Council (PSC) – Cyber S&T Roadmap**
  - Identified M&S as a key cross-cutting technology area and gap for S&T
  - 2014 Community of Interest (COI) update to the Cyber S&T Roadmap, confirms that M&S is still a significant gap for cyber S&T
- **Feb 2011 and Jun 2013 CJCS execute order to "Incorporate realistic cyberspace conditions into major DoD exercises"**
- **CJCS Notice 3500.1 – 2013-2016 Chairman's Joint Training Guidance**
- **2013 ASD(R&E)-directed Cyber M&S Campaign (CMSC) Report**
  - Presented roadmap for advancement of cyber M&S capabilities
  - Identified several areas for pilot efforts
- **2013 Cyber Investment Management Board (CIMB) S&T Landscape Analysis**
  - Reiterated modeling mission dependencies from cyber as a key gap
- **2014 USCYBERCOM/J9 S&T Strategy**
  - Identifies M&S model environments for mission planning, experimentation, testing, training, and exercise as a critical focus area
- **2015 DoD Cyber Strategy**
  - Specifically states need for "enterprise-wide cyber modeling and simulation capability"
  - M&S should support persistent training environments, force assessment, planning, exercises

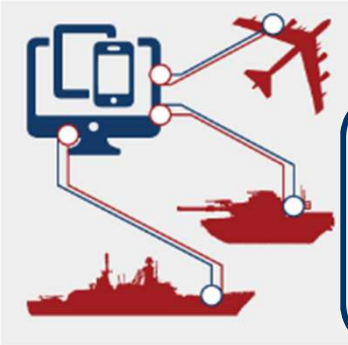
2015 Cyber Defense Strategy

The purpose of this strategy is to guide the development of DoD's cyber forces and strengthen our cyber defense and cyber deterrence posture. It focuses on building cyber capabilities and organizations for DoD's three primary cyber missions.

DoD's Three Primary Cyber Missions:

Defend DoD networks, systems, and information

Defend the U.S. homeland and U.S. national interests against cyberattacks of significant consequences



Provide cyber support to military operational and contingency plans

Figure is UNCLASS

- **Strategic Goals:**
  - Build and maintain ready forces and capabilities to conduct cyberspace operations.
  - Defend the DoD information network, secure DoD data, and mitigate risks to DoD missions
  - Be prepared to defend the U.S. homeland and U.S. vital interests from disruptive or destructive cyberattacks of significant consequence
  - Build and maintain viable cyber options and plan to use those options to control conflict escalation and to shape the conflict environment at all stages
  - Build and maintain robust international alliances and partnerships to deter shared threats and increase international security and stability

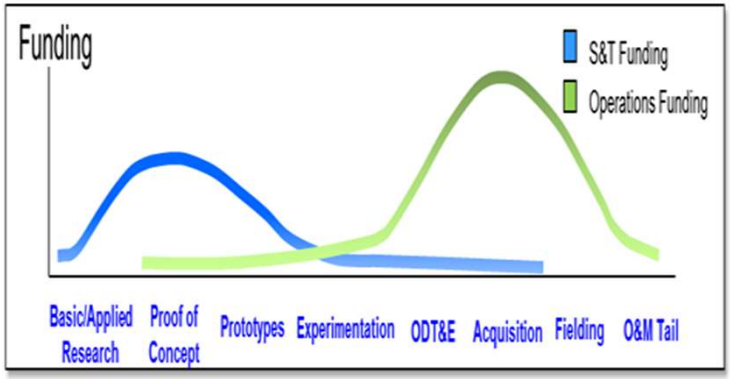
Source: http://www.defense.gov/News/Special-Reports/0415_Cyber-Strategy

Accelerate Innovative Cyber R&D

What

The Defense Department will continue to **accelerate innovative cyber research and development to build cyber capabilities**. The DoD **research and development community** as well as established and emerging private sector partners **can provide DoD and the nation** with **a significant advantage in developing leap-ahead technologies** to defend U.S interests in cyberspace. DoD will focus its Science & Technology (S&T) to develop new cyber capabilities to support emerging DoD cyber objectives and to increase the effectiveness of the CMF and the broader DoD cyber workforce.

Why



"America's economic prosperity, national security, and our individual liberties depend on our commitment to securing cyberspace and maintaining an open, interoperable, secure, and reliable internet."

"The challenges [in cyberspace] are so broad…it is going to take a true partnership between the private sector, the government and academia to address them [them]."

How

- Establish a Cyber Research Development and Acquisition Command
- Cyber Transition to Practice
- Tighten Interaction between S&T and Operational Community
- Engage Industry

Engage Industry

- ***Desired End State:***
  - Non-traditional industry members are engaged and their ideas for game-changing approaches are fully leveraged
  - Industry's best R&D talent is accessible to the DoD in new and flexible ways
  - Investments made outside the DoD are fully leveraged
- ***Accomplishments:***

RAPID REACTION Technology Office

- Establish an S&T outreach effort that enables industry to bring forward game changing ideas; Leveraging the Innovation Outreach Program and hosting a Cyber Needs Workshop to be followed by the Solutions Workshop (June)

ITEP

- Establish an exchange program with industry experts to make additional talent accessible; Leveraging the DoD CIO Information Technology Program (ITEP) to facilitate an exchange DoD S&T persons with industry and vice versa

CSIAC

- Leveraging Computer Security & Information System Information Analysis Center (CSIAC) to organize workshops on key areas the Department can use help from industry

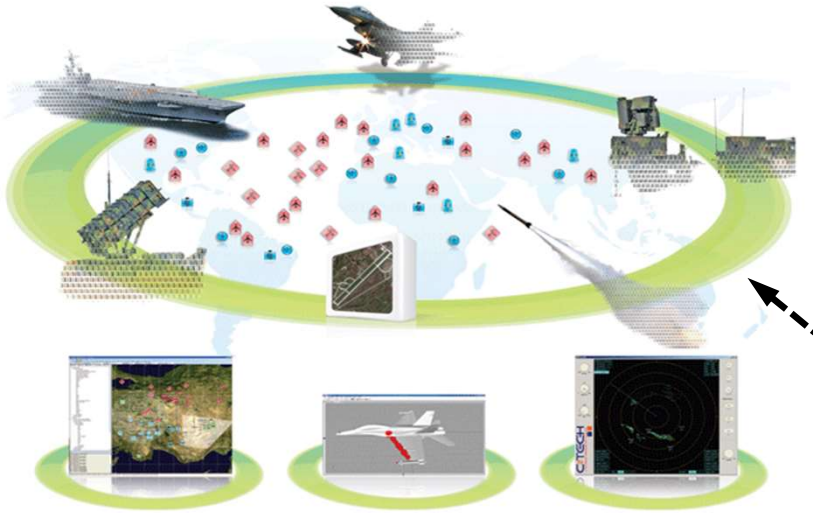
DEFENSE INNOVATION UNIT EXPERIMENTAL

- The mission of DIUx is technology scouting and to serve as the point of entry for non-traditional (e.g., start-up, small business, etc.) high tech companies to access DoD's acquisition and operational communities for products that are ready for transition

Supporting Efforts to Advance Cyber M&S

- **Identifying plan for developing enterprise cyber M&S capability**
- **Used earlier Cyber M&S Campaign Report as a starting point for scope of capabilities needed and current state**
- **Working with user/developer communities of interest to determine current capabilities and needs for cyber M&S**
  - Research & Engineering (lead: Cyber COI)
  - Force Structure & Programming Analysis (lead: JS 5/8)
  - Acquisition/T&E (lead: AT&L)
  - Mission Planning & Support (lead: USCYBERCOM)
  - Education & Training (lead: JS J7)
- **Results will feed into POM Issue Paper to request funding to accelerate cyber M&S development**

Cyber Operational Architecture Training System (COATS



Traditional Battle Staff Training Environment

- Conventional terrain-based military combat M&S interfaced w/ operational C4I systems
- Operational/strategic level of war
- Minimal M&S of cyber network layers/effects
- "White cards" typically used to inject cyber effects to the battle staff training audience

Target Damage Adjudication

Cyber Training Environment

- Cyber ranges and M&S with C4I systems & infrastructure serving as key terrain
- Tactical/operational level of war
- Minimal M&S of kinetic and environmental effects
- Closed loop cyber range runs independently from traditional environment

Summary

- **Enduring Activities:**
  - USCC R&D Organization
  - Continue to transition emerging Cyber S&T into more operationally mature capabilities
  - CIL – continuing relationship between USCYBERCOM/S&T community
  - Continued engagement w/ industry
  - DoD's Cyber S&T Community of Interest and ASD(R&E) Information System & Cyber Technologies office outreach will continue engagements established by LOE 2-8-1
- **Engaged multiple cross-DoD initiatives and partners:**
  - DASD EC&P Rapid Reaction Technology Office (RRTO) Innovation Outreach – *Sponsored workshop soliciting novel technology solutions from industry*
  - DoD CIO Information Technology Exchange Program (ITEP) – *Information exchange*
  - USCYBERCOM – *Collaborated to leverage use of CIL*
  - Army Cyber (ARCYBER) – *Supported dynamic cyber defense training efforts*
  - DIUx – *Explored options for novel innovative solutions*
  - LOE 1 & 2 – *Identified synergy between objectives that could be leveraged*
  - Cyber Security and Information Systems Analysis Center (CSIAC) – *Information exchange with non traditional industry members*