

UNCLASSIFIED



Defense Cyber S&T Strategies & Initiatives

DoD/DHS Small Business Innovation Research Workshop

23 July 2013

Dr. Steven King
Deputy Director, Cyber Technology
Office of the Assistant Secretary of Defense
(Research and Engineering)

UNCLASSIFIED



UNCLASSIFIED

S&T Influencing the DOD Cyber Landscape



“...we will continue to invest in capabilities critical to future success, including... operating in anti-access environments; and prevailing in all domains, including cyber.”

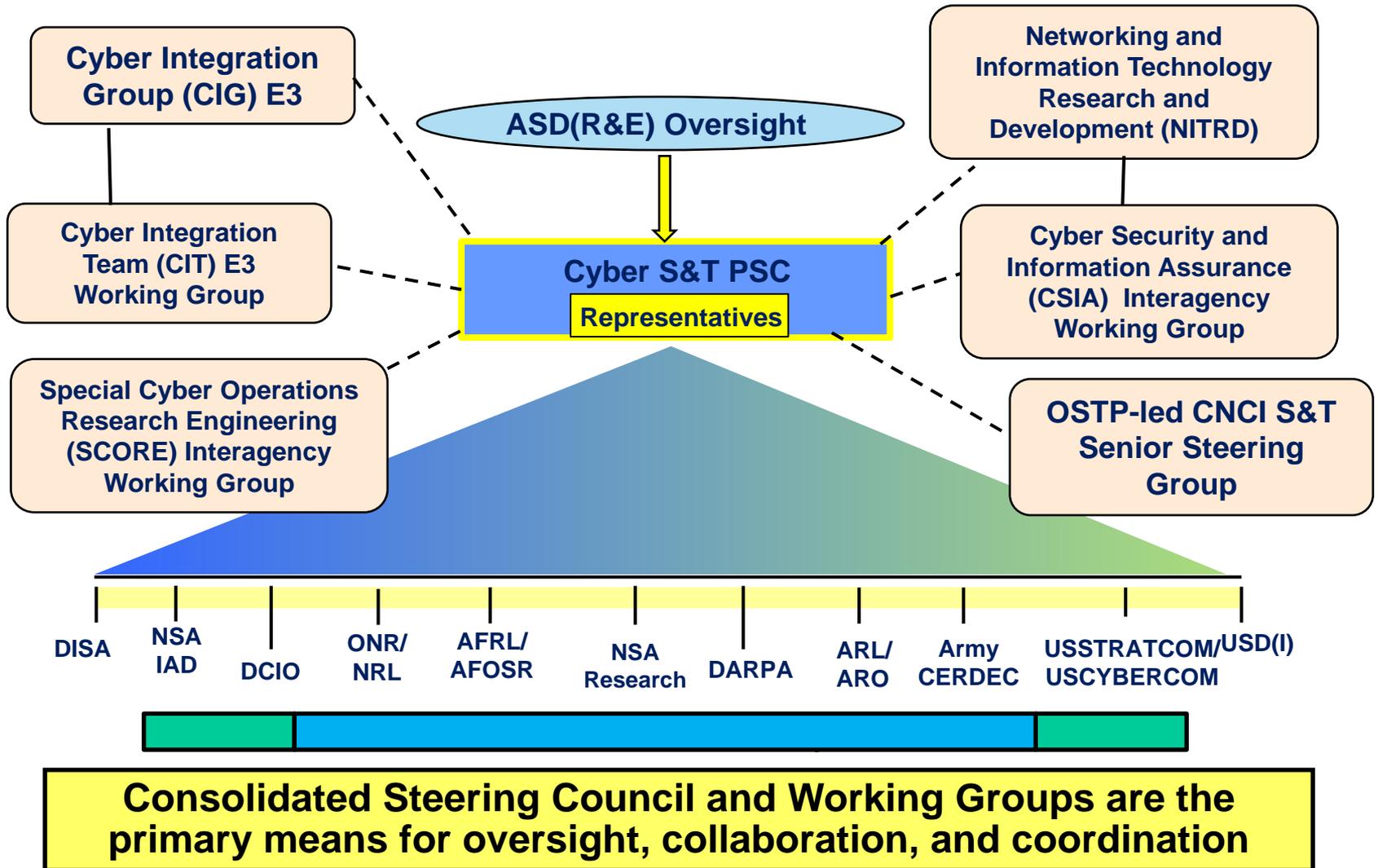
- President Obama, January 2012.



UNCLASSIFIED



DoD Cyber S&T Coordination (U)





UNCLASSIFIED



CYBER PSC S&T ROADMAP

UNCLASSIFIED



Cyber Priority Steering Council Research Roadmap Problem Statement



Problem: DoD lacks agile cyber operations and resilient infrastructure to assure military missions

- **Cyber-dependent systems are increasingly complex, making them more susceptible to attack and more difficult to reliably defend**
 - Reliance on globalized commercial hardware and software compromises our underlying cyber infrastructure
 - Current trust management and operational assurance approaches do not adequately scale
- **Commanders lack real-time situational awareness and an understanding of the mission impact of events in the cyber domain**
 - Commanders operational decision tradespace is limited as a result
 - Commanders currently have limited ability to evaluate and manage operational risk of cyber assets and actions – local decisions can have a global impact
- **Adversaries exploit severe asymmetric advantages in cyberspace**
 - A single vulnerability may enable widespread compromises
- **Lack of quantitative metrics and measures for cyber inhibits improvements in the agility of cyber operations and the resiliency of cyber infrastructure**



Key Capability Areas

Embedded, Mobile, and Tactical Systems (EMT)

Assuring Effective Missions

Assess and control the cyber situation in mission context

Agile Operations

Dynamically reshape cyber systems as conditions/goals change, to escape harm



Resilient Infrastructure

Withstand cyber attacks, and sustain or recover critical functions

Trust

Establish known degree of assurance that devices, networks, and cyber-dependent functions perform as expected, despite attack or error

Cyber Modeling, Simulation, and Experimentation (MSE)

(MSE & EMT) cross-cutting areas in analysis of Joint Chiefs of Staff Cyber Gaps



SERVICE CYBER STRATEGIES



Air Force Cyber Vision 2025

Key Thrusts



U.S. AIR FORCE

- **Assure and Empower the Mission (MAJCOMs)**
 - Assure national security missions to security standards exceeding biz systems
 - More effective use of Title 10/50/32
 - Multi-domain synch/integrated effects
 - Increase cost of adversary OCO
- **Improve Cyber Education, Accessions, ACE (AETC, A1, A6, AFSPC)**
- **Advance Processes (AFPSC, AQ, TE, MAJCOMS)**
 - Require/design in security; secure full life cycle
 - Rapid, open, iterative acquisition; engage user/test early
 - Integrate cyber across CFMPs
 - Advance partnerships, align funding
- **Enhance Systems and Capabilities (AFSPC, AQ, AFMC)**
 - Reduce complexity, verify systems
 - Hardened, trusted, self-healing networks and info
 - Agile, resilient, disaggregated mission architectures
 - Real-time cyber situational awareness/prediction, managed information objects, cyber FME
- **Focused, Enabling S&T (AFRL)**
 - Assure and empower missions
 - Enhanced agility & resiliency
 - Optimize human/machine systems
 - Establish foundations of trust

OCO = Offensive Cyberspace Operations; ACE = Air Force Cyber Elite; FME = Foreign Material Exploitation



Navy Cyber Power 2020

Technology Innovation - Strategic Initiatives

- **Deliver cyber SA**
 - Correlate, assess, and integrate timely and operationally relevant cyber information into the operational pictures of Navy and Joint commanders
- **Lead Joint cyber modeling, simulation and analysis**
 - Focus on establishing the capability to model offensive cyberspace operations, estimate collateral damage, and analyze impact after delivery in a manner similar to MS&A capabilities for conventional ordnance
- **Pilot new technology**
 - Institute a robust pilot program to aggressively seek out and test emerging cyber technologies in real world and cyber ranges, assess their operational impact, and be able to rapidly integrate across the Navy

Leverage industry, academia, Allies and Joint partners to rapidly update Navy cyberspace capabilities to stay ahead of the threat



UNCLASSIFIED

Army Strategic Planning Guidance 2013



- **Given the heavy reliance on military computer networks and critical infrastructure, it is essential that the Army be able to defend key systems and ensure the continuity of critical network functions in the face of disruption.**
- **The mission to defend our network is a priority.**
 - First, the Army's network must be built, operated and maintained in a defensible manner informed by cyberspace forces while continuing to enable mission command.
 - Second, defensive cyber capabilities are essential to all Army operations, with cyber warriors integrated into organizations and unit staffs that support the Joint warfighter all the way down to the Army's tactical edge.
 - Finally, when appropriately authorized, the Army must be prepared to plan and conduct cyberspace operations consistent with applicable statutes and National Command Authority directives.
- **Provide modernized and ready, tailored land force capabilities to meet combatant commanders' requirements across the range of military operations.**
 - The Army will pursue a capability set management construct for the Network that will cut across functional areas and focus on three primary objectives: building capacity, improving security and delivering enterprise services to the entire force.

Source: http://www.defenseinnovationmarketplace.mil/resources/army_strategic_planning_guidance2013.pdf

UNCLASSIFIED



UNCLASSIFIED

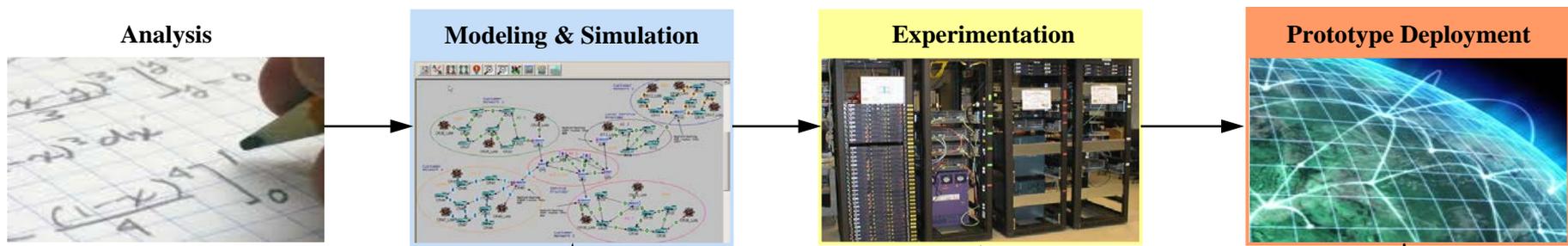


NEW INITIATIVES

UNCLASSIFIED



Approaches to Cyber Assessment

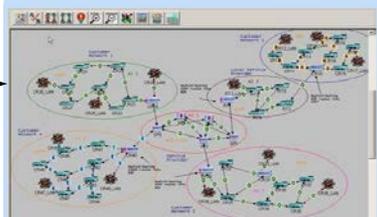


Analysis



- Based on first principles
- Develops global performance intuition
- Provides bounds that serve as implementation goals
- Provides corner cases to validate modeling, simulation, and emulation

Modeling & Simulation



- Fidelity/complexity/time trade-off
- Repeatable
- Easiest transfer across organizations

Experimentation



- Real code, real apps, emulated environment
- Repeatable
- Provide uses with a real time implementation for evaluation

Prototype Deployment



- Validates modeling, simulation, and emulation
- Difficult to repeat
- Difficult to obtain ground truth

	Analysis	Modeling & Simulation	Experimentation	Prototype Deployment
Fidelity	Low	Low	Moderate to High	High
Scalability	High	High	Moderate	Low
Cost	Low	Low	Moderate	High
Repeatability	N/A	High	Moderate to High	Low
Program Phase	Early	Early	Mid-term	Mid-term to Late

Selecting an appropriate combination of assessment approaches is critical to a successful quantitative evaluation



Cyber Measurement Campaign

Long-term Strategy Development

- Develop plan to incorporate quantitative assessment into cyber S&T
- Recommend strategy to develop & use experimentation ranges

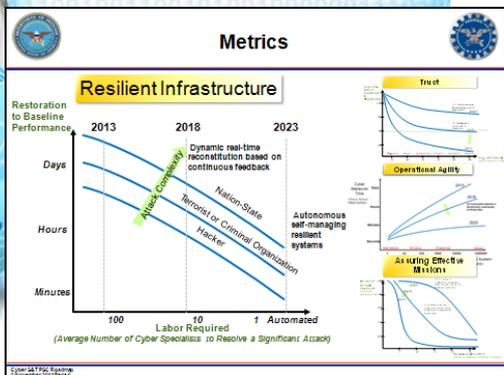
Experimentation

- Test Cyber PSC concepts of cyber resiliency and agility in a specific context and measure their impact on security
- Initial input for long-term experimental techniques and metrics

Cyber Testbed and Range Assessment

- Create range inventory as a cyber S&T community resource
- Identify gaps in current range capabilities for testing of future S&T

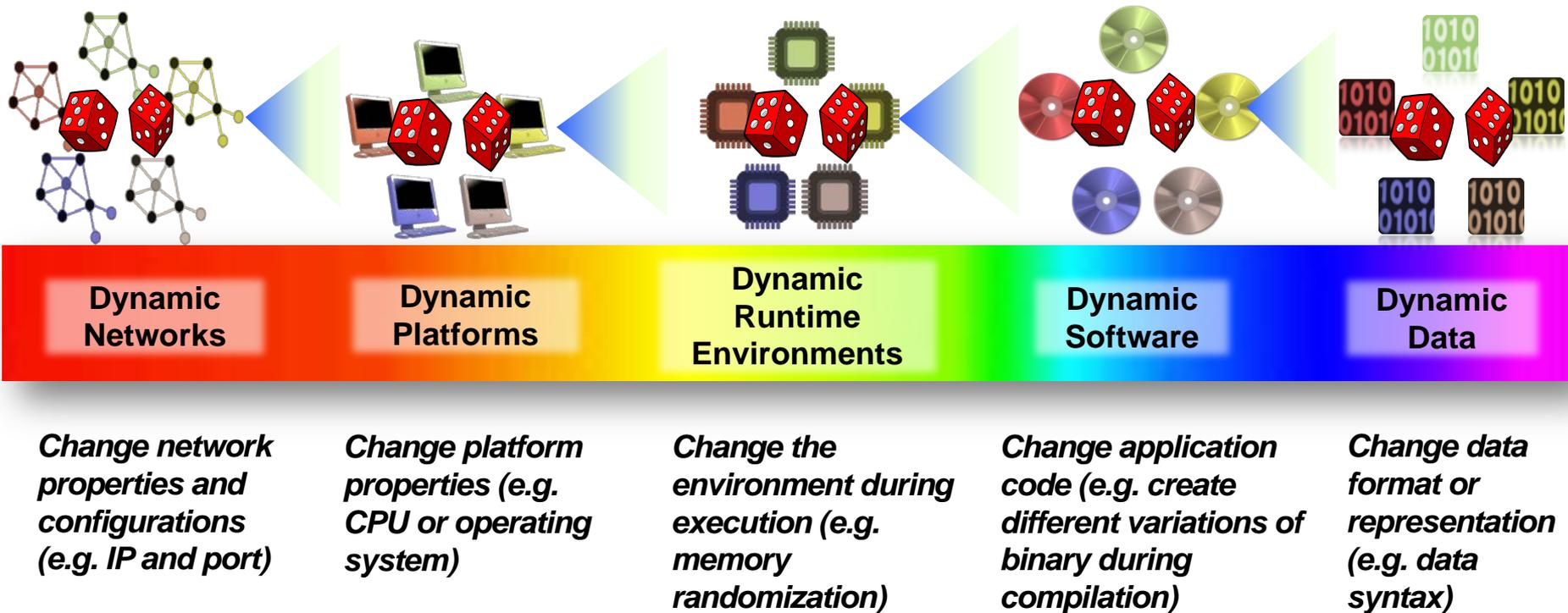
- **Impact:** Improved metrics and quantitative analysis of tools and techniques to enable evaluation of S&T investments prior to deployment; technology assessments that correspond to real world conditions; strategic approach to DoD Range investment.
- **Transition:** Work with DT and TRMC to develop seamless experimentation, developmental testing and evaluation to enable rapid insertion of cyber tools into live networks.





Cyber Moving Target Approaches

- A broad range of techniques are proposed for moving target
- Each technique category requires its own metrics and experimental methods

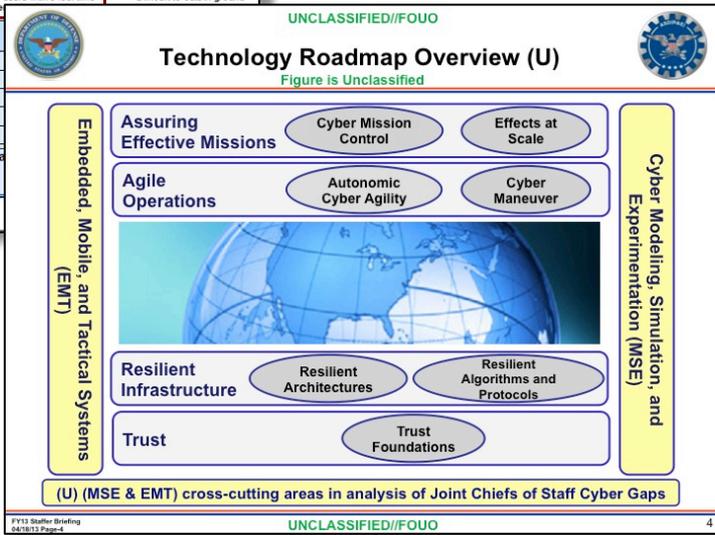
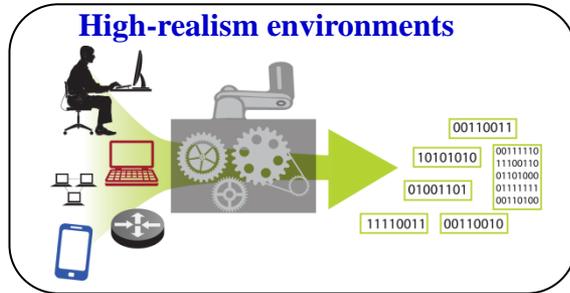
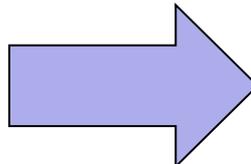
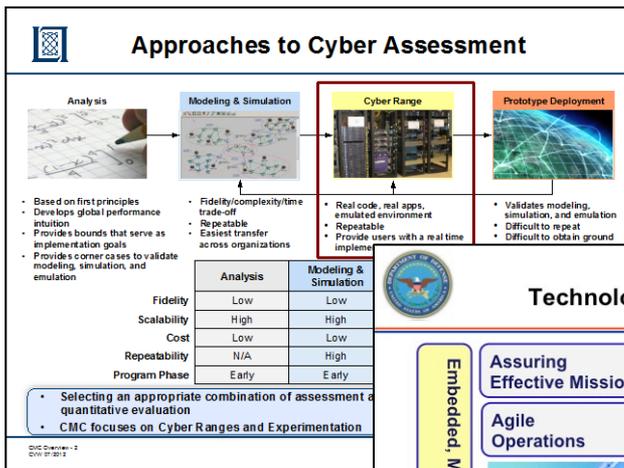




Cyber Modeling and Simulation Campaign

Objective:

- Recommend a strategy to shape the development of future cyber M&S capabilities





UNCLASSIFIED



OUTREACH

UNCLASSIFIED



UNCLASSIFIED

DoD Cyber SBIRs *Outreach to Small Businesses*



- **DoD Small Business Innovative Research (SBIR) and Small Business Technology Transfer (STTR) program in cyber**
 - Harness talent of small technology companies to meet U.S. military needs – can team with Universities
 - Potential for commercialization or transition to DoD of successful research
 - Awards up to \$150K for Phase I projects (+ \$1.0 M for Phase II)
- **FY12 – today: sponsored 67 SBIR projects focusing on Cyber Research (~\$13.9M)**
- **Going forward, SBIR Topics will reflect the goals of the Roadmap**
 - Foundations of Trust
 - Resilient Infrastructure
 - Agile Operations
 - Assuring Effective Missions

Source: <http://www.dodsbir.net>

UNCLASSIFIED



Open Broad Agency Announcements

- **Army Research Office (ARO)** (<http://www.arl.army.mil/www/default.cfm?page=8>)
 - Solicitation #:W911NF-12-R-0012; BAA for Basic and Applied Research, Section II.A.1.C
- **Army Research Laboratory (ARL)** (<http://www.arl.army.mil/www/default.cfm?page=8>)
 - Solicitation #:W911NF-12-R-0010 ; BAA for Advanced Computing Initiative (ACI)
- **Office of Naval Research (ONR)** (<http://www.onr.navy.mil/en/Contracts-Grants/Funding-Opportunities/Broad-Agency-Announcements.aspx>)
 - Solicitation #: ONRBAA12-00; BAA for Long-Range Broad Agency Announcement for Navy and Marine Corps Science and Technology 12-001
- **Naval Research Laboratory (NRL)** (<http://heron.nrl.navy.mil/contracts/baa/index02.htm>)
 - Solicitation #: 55-11-01; Information management and decision architectures
 - Solicitation #: 55-11-02; Mathematical foundations of high assurance computing
 - Solicitation #: 55-11-03; High assurance engineering and computing
 - Solicitation #: 55-11-04; Advanced naval network solutions
 - Solicitation #: 55-11-05; Adversarial modeling and decision support
 - Solicitation #: 55-11-06; Software engineering for high assurance computer systems
- **Air Force Office of Scientific Research (AFOSR)** (<http://www.grants.gov/search/search.do>)
 - Solicitation #: BAA-AFOSR-2012-0001
- **Defense Advanced Research Projects Agency (DARPA)** (http://www.darpa.mil/Opportunities/Solicitations/DSO_Solicitations.aspx)
 - Solicitation #: DARPA-BAA-11-65; Defense Sciences Research and Technology

***Small Business Innovation
Research Announcements***
<http://www.dodsbir.net>

NSA Contact Information
(No Open BAAs)

Acquisition Resource Center
 Phone: (443)-479-9572
 E-mail: nsaarc@nsaarc.net
 Office of Small Business Programs
 Phone: (443)-479-9572
 E-mail: nsaarc@nsaarc.net



Accelerating Transition to Practice

**There is a strong need to move technology out of labs.
How can we improve transitions from SBIRS?**

- **Federal CS Research Plan**

- http://www.nitrd.gov/fileupload/files/Fed_Cybersecurity_RD_Strategic_Plan_2011.pdf

- **Interagency Coordination**

- Cyber Security and Information Assurance (CSIA) Interagency Working Group (IWG)
- CSIA Senior Steering Group (CNCI Initiative 4)
- Special Cyber Operations Research and Engineering IWG (CNCI Initiative 4)

- **A focus on transition**

- Technology Discovery
- Test and Evaluation
- Transition, Adoption, and Commercialization



UNCLASSIFIED

Back-up



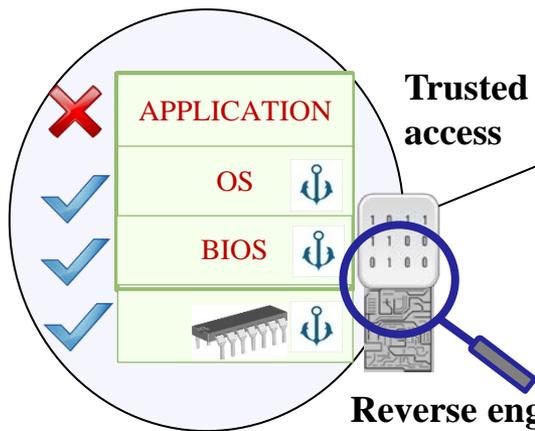
UNCLASSIFIED



Trust

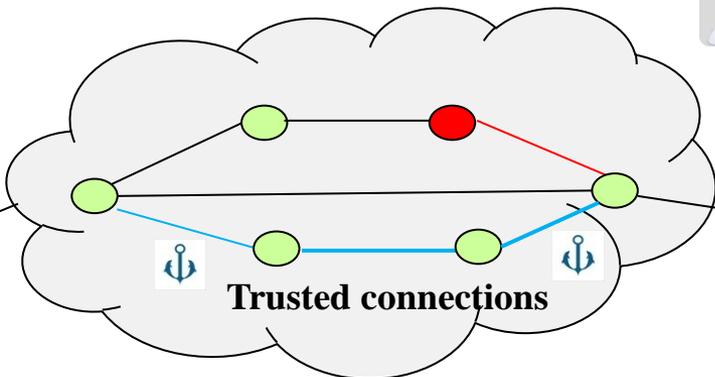
Technical Challenges and Research Opportunities

Trusted boot and operations



Reverse engineering and forensics

Trusted access



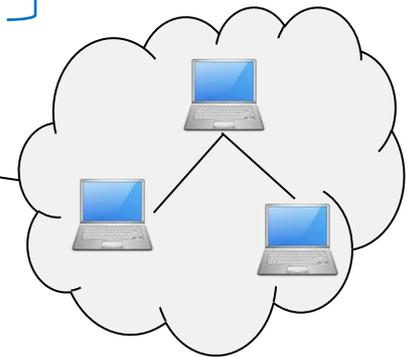
Trusted connections

Recommenders



Reputation management system

Trust Token



Trusted organization

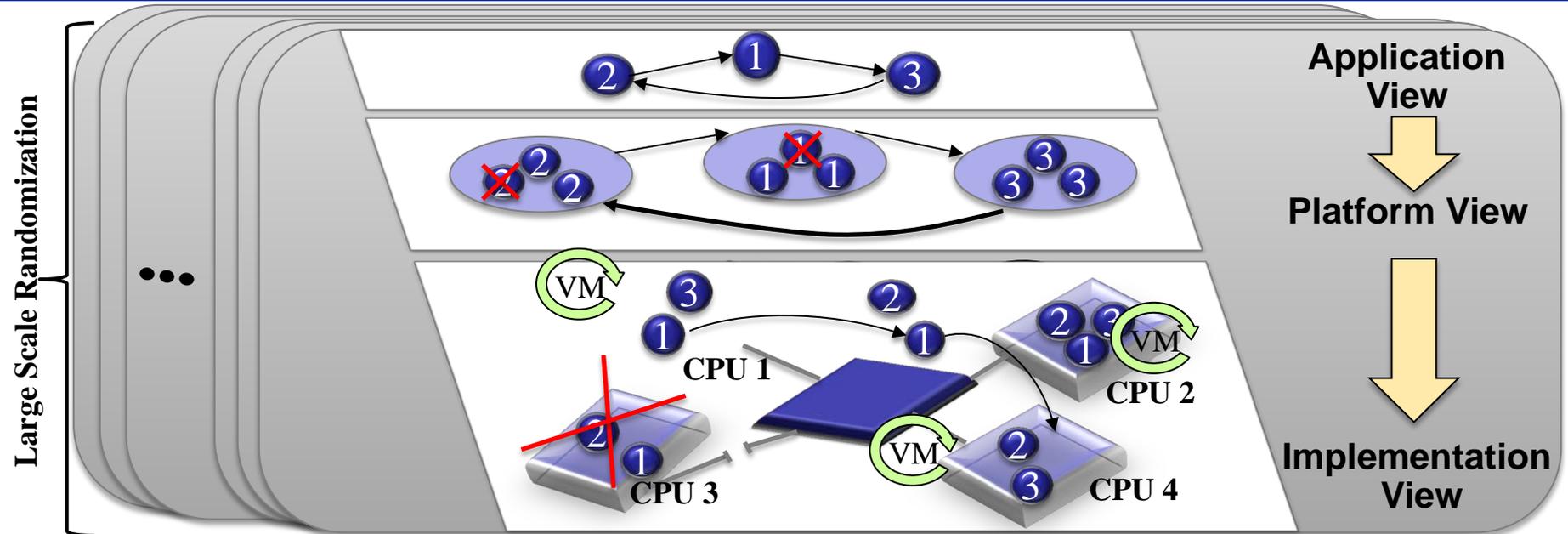
Trust Foundations

- Scalable reverse engineering and analysis
- Trust establishment, propagation, and maintenance techniques
- Measurement of trustworthiness
- Trustworthy architectures and trust composition tools



Resilient Infrastructure

Technical Challenges and Research Opportunities



Resilient Architectures

- Resiliency for operational systems
- Mechanisms to compose resilient systems from brittle components
- Integration of sensing, detection, response, and recovery mechanisms
- Secure modularization and virtualization of nodes and networks
- Resiliency-specific modeling and simulation

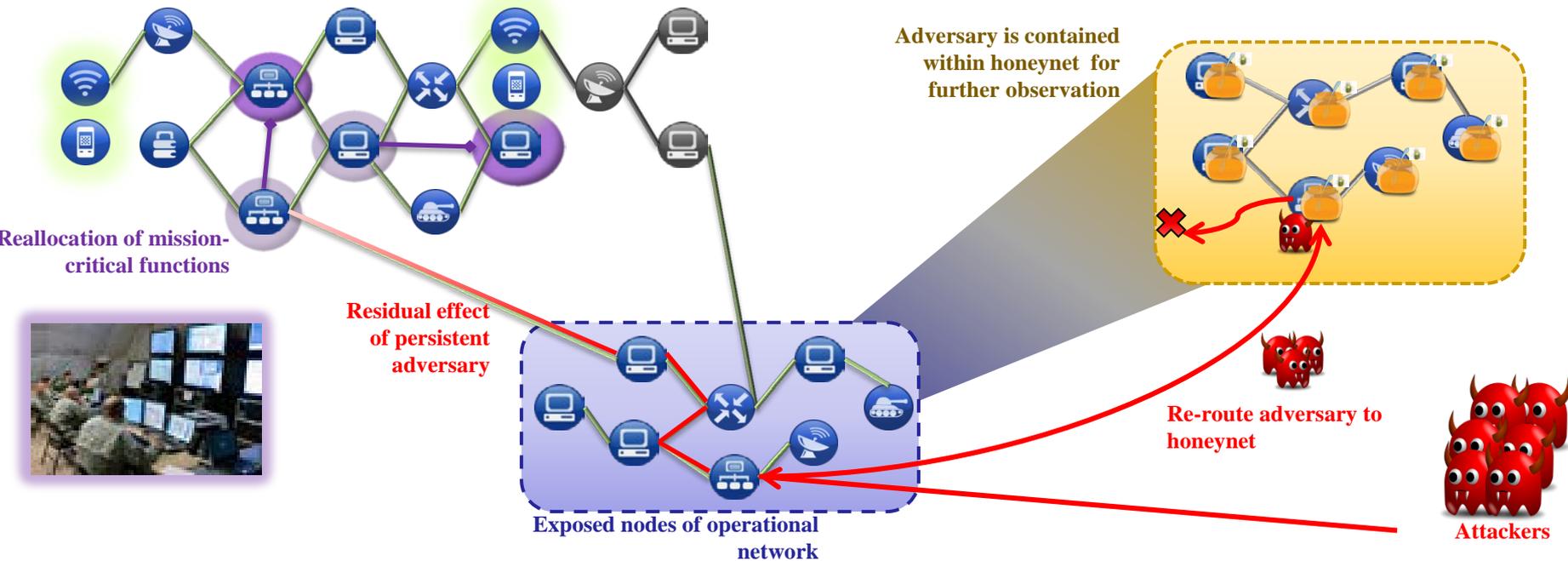
Resilient Algorithms and Protocols

- Code-level software resiliency
- Network overlays and virtualization
- Network management algorithms
- Mobile computing security



Agile Operations

Technical Challenges and Research Opportunities



Autonomic Cyber Agility

- Techniques for autonomous reprogramming, reconfiguration, and control of cyber components
- Machine intelligence and automated reasoning techniques for executing courses of action

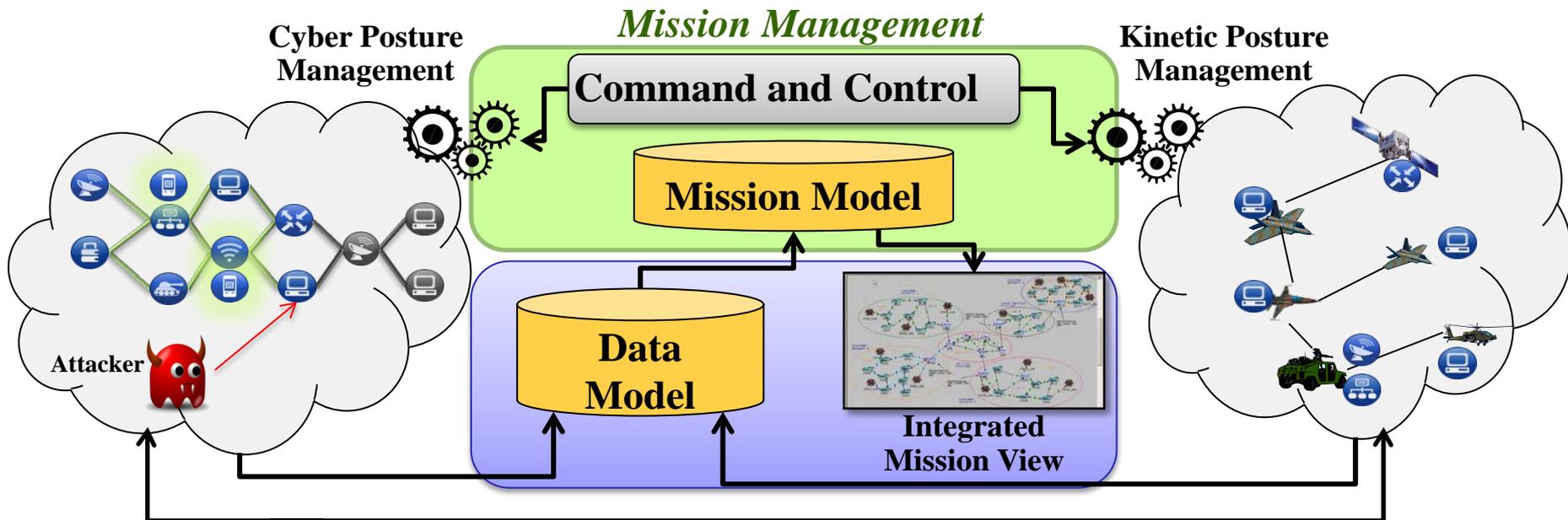
Cyber Maneuver

- Distributed systems architectures and service application polymorphism
- Network composition based on graph theory
- Distributed collaboration and social network theory



Assuring Effective Missions

Technical Challenges and Research Opportunities



Mission Situational Awareness

Cyber Mission Control

- Techniques for mapping assets and describing dependencies between mission elements and cyber infrastructure
- Techniques for course of action development and analysis
- Cyber effects assessment