



National and Defense S&T Strategies & Initiatives

DoD/DHS Small Business Innovation Research Workshop

25-26 July 2012

Steven King, Ph.D.

Deputy Director for Cyber Security Technologies

Research Directorate, Information Systems & Cyber Security

Office of the Assistant Secretary Defense for Research and Engineering



Outline



- **Key Capability Areas/Objectives**
- **Cyber Metrics**
- **Tech Challenge Areas Research Approaches**
- **OSD SBIR Activities In Cyber**



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 10 Year Objectives

Vision

10 Year Objective

<p>Assuring Effective Missions</p>	<p>Can track infrastructure state and cyber attacks, understand and predict how they affect mission functions</p>	<ul style="list-style-type: none"> • <i>Predictive cyber/kinetic mission tools integrating historical data, situational awareness, and simulation techniques for use during live mission execution</i>
<p>Agile Operations</p>	<p>Infrastructure allows systems and missions to be reshaped nimbly to meet tactical goals or environment changes</p>	<ul style="list-style-type: none"> • <i>Time-constrained automated control loops for fast-paced cyber campaigns and real-time course of action management</i> • <i>Temporal-spatial coordination of network, system, and application reconfiguration for maneuver</i>
<p>Resilient Infrastructure</p>	<p>Missions are difficult to disrupt even with successful cyber attack</p>	<ul style="list-style-type: none"> • <i>Autonomous self-managing resilient systems</i> • <i>Mobile devices with fully attested hardware, firmware, and applications</i>
<p>Trust</p>	<p>Quantitative trust in systems as built and in operation; systems of known trust from elements of mixed trust</p>	<ul style="list-style-type: none"> • <i>Trusted systems from components of mixed trust</i>



Overarching Cyber Metric Work Factor Ratio

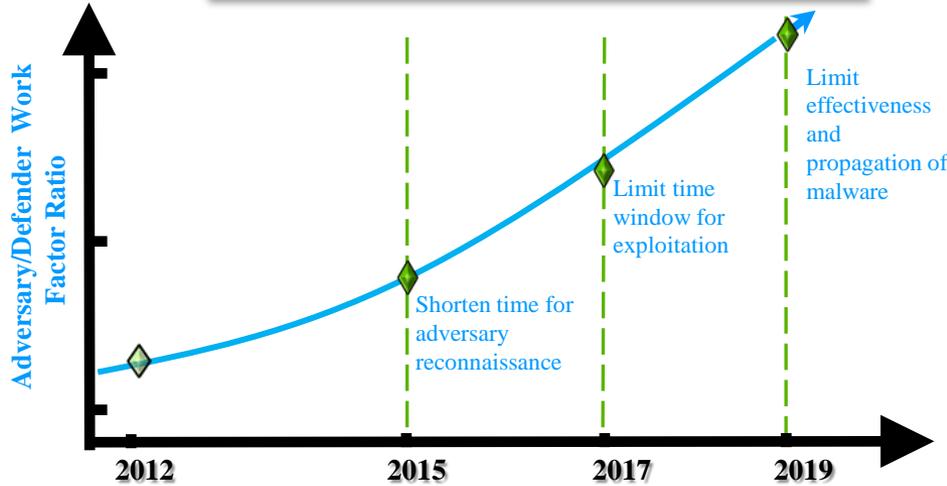
• Missions

- Kinetic, cyber, and combined missions will have a cyber dependency

• Infrastructure

- Any element of the cyber infrastructure may be compromised and manipulated
- DoD will continue to leverage commercial products and services we do not own or control
- DoD infrastructure defies establishing an all-encompassing static perimeter

Challenge:
*Increase Adversary / Defender
Relative Work Factor Over Time*



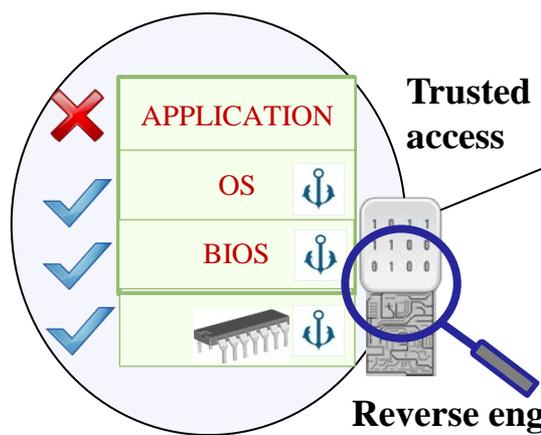
Perimeter is not well defined



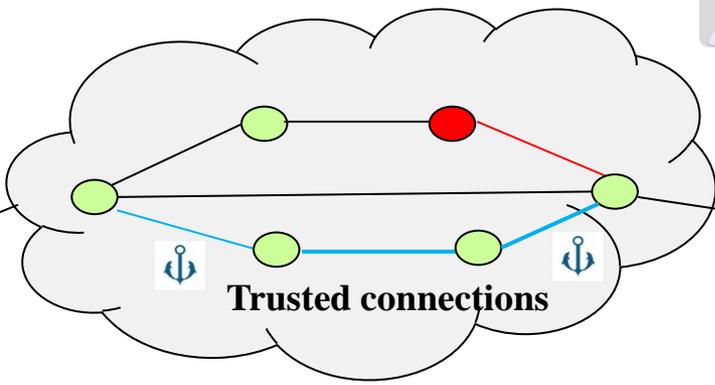
Trust

Technical Challenges and Research Opportunities

Trusted boot and operations



Trusted access

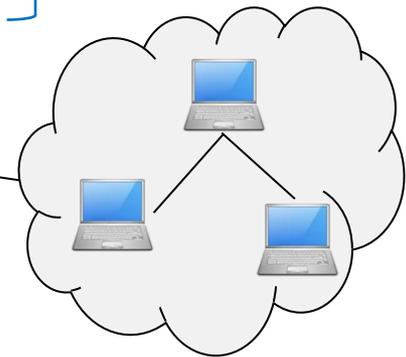


Recommenders



Reputation management system

Trust Token



Trusted organization

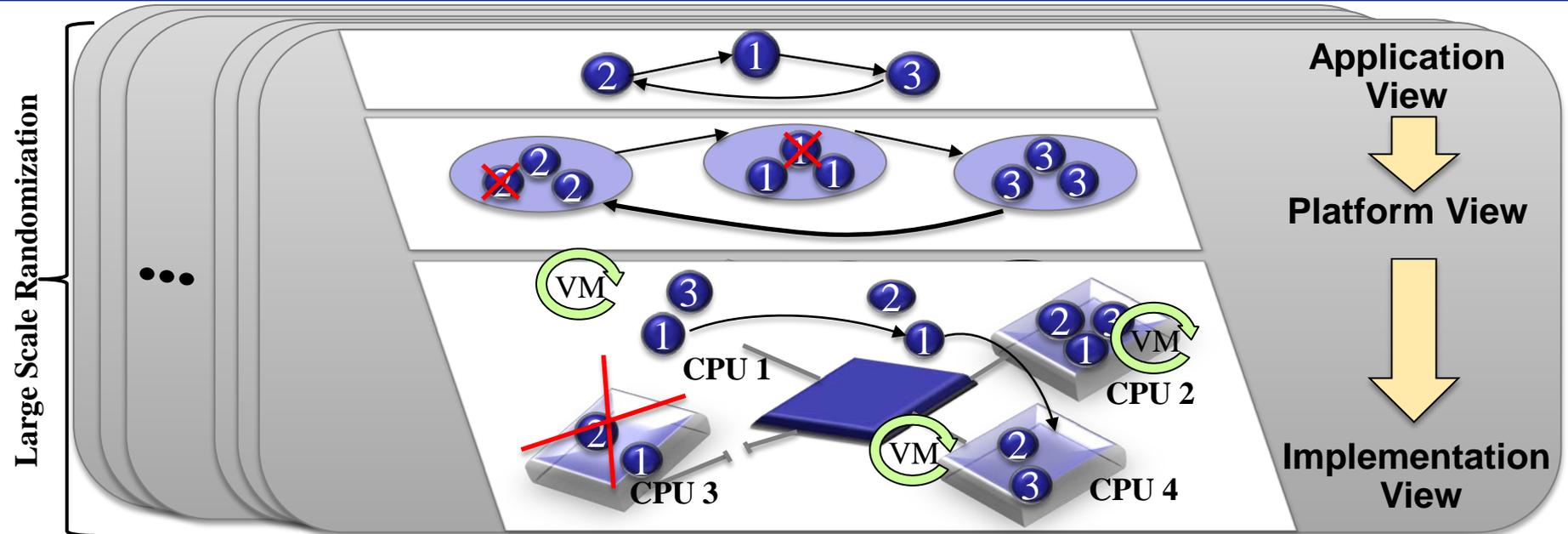
Trust Foundations

- 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

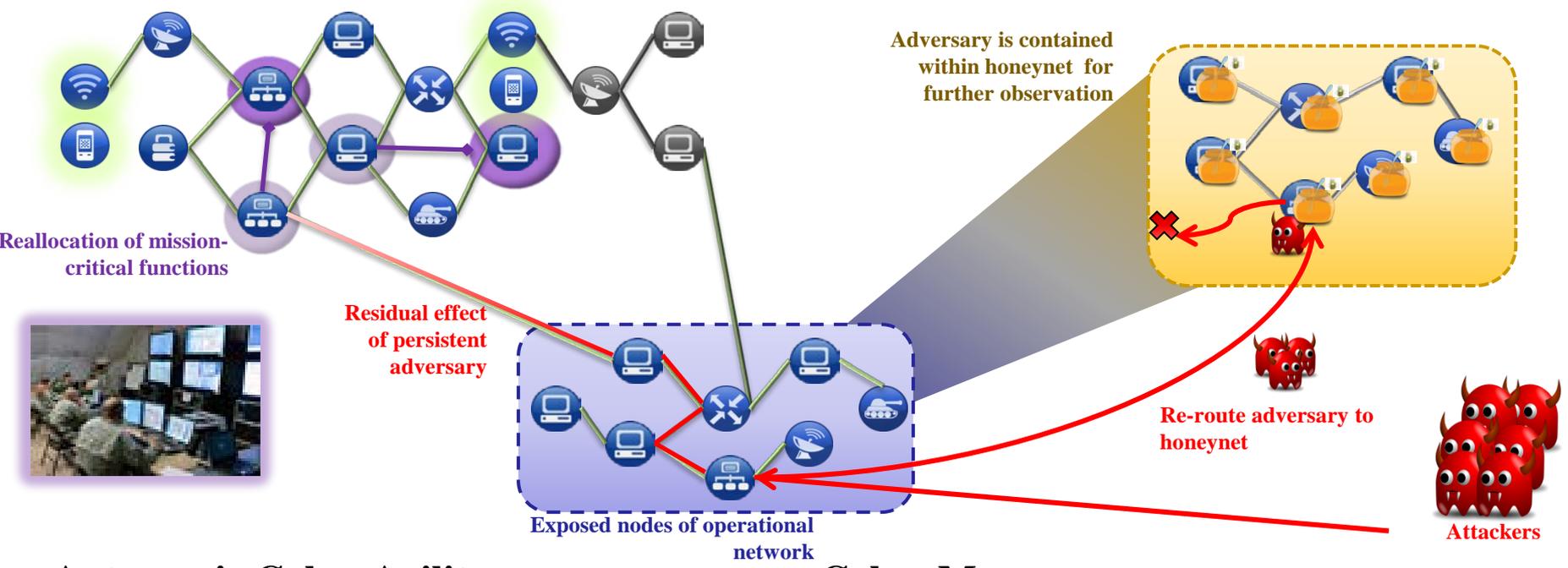
Resilient Algorithms and Protocols

- 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

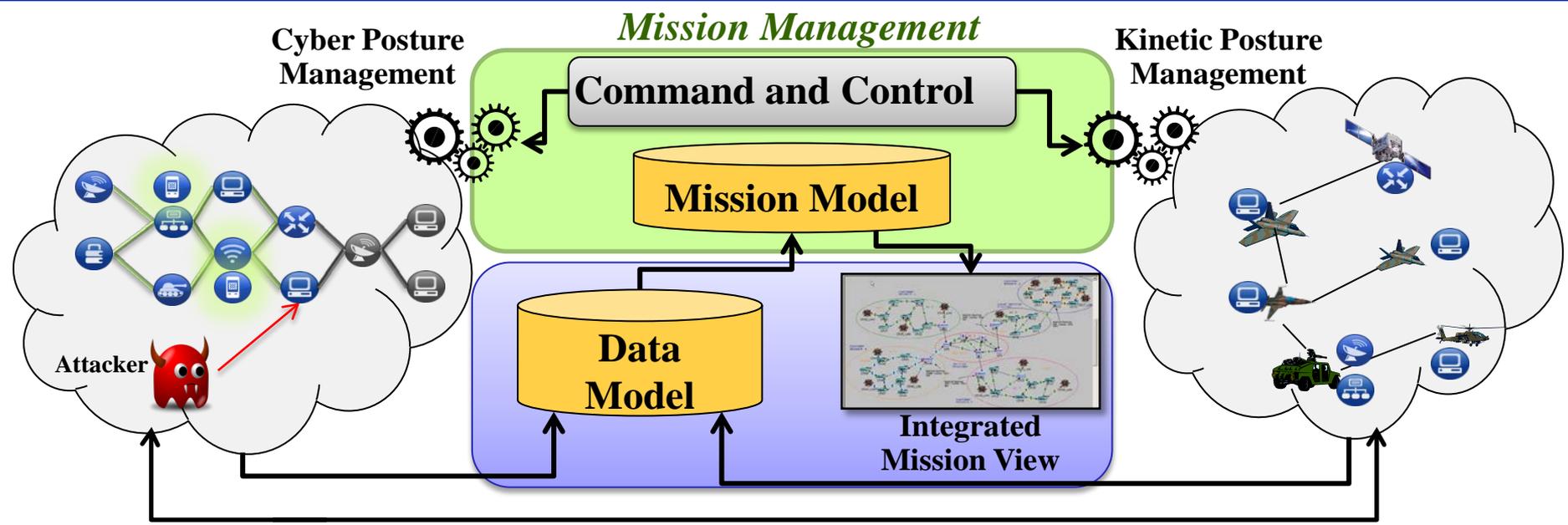
Cyber Maneuver

- 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

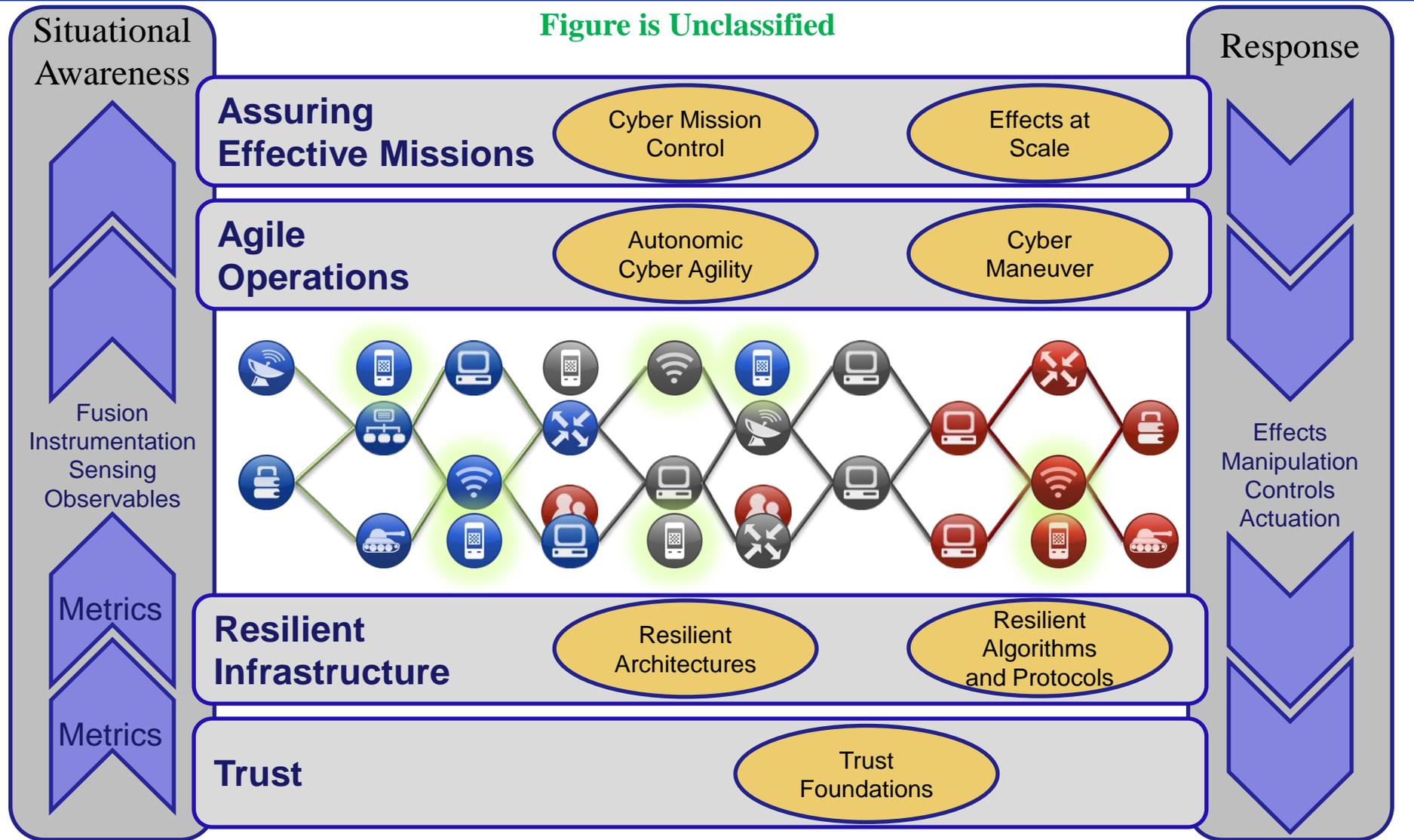
Cyber Mission Control

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



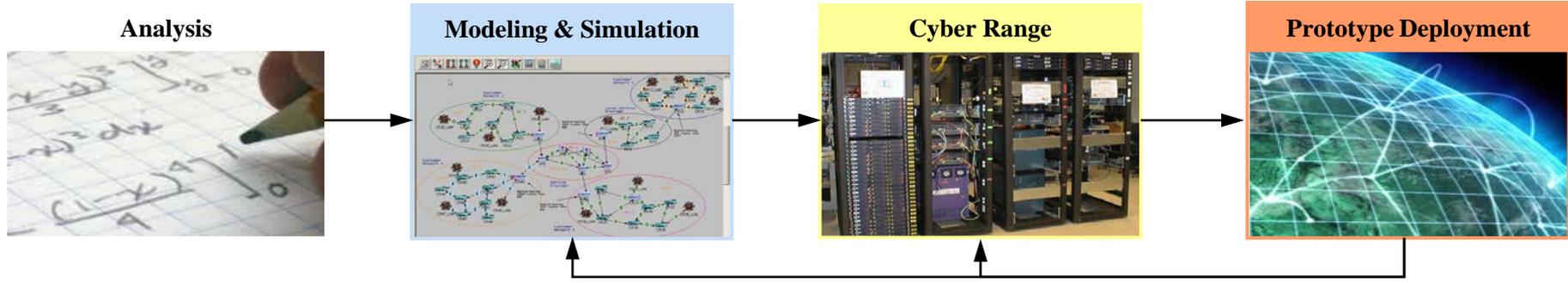
Technology Challenge Summary

Figure is Unclassified





Approaches to Cyber Assessment



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

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

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

	Analysis	Modeling & Simulation	Cyber Range	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

Cyber PSC oversight / Performers: MIT LL & AFRL



Long-term Strategy Development

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

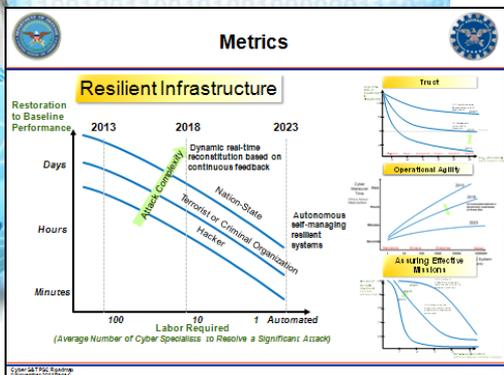
Experimentation

- 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.





DoD Cyber SBIRs Overview



- **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
 - Potential for commercialization or transition to DoD of successful research
 - STTR funds joint company/research institution R&D
 - Awards up to \$150K for Phase I projects (over 1 year)
 - Awards up to \$1.0 M for Phase II projects (over 2 years)
- **Cyber SBIR Topics.** Currently sponsoring 85 SBIR projects focusing on Cyber Research (~\$13M)



DoD Cyber SBIRs Overview

- **ASD(R&E) Cyber SBIR/STTR Projects**

- Focus on cyber security starting in 2005
- FY 2011
 - 6 new cyber topics approved; 21 new projects
 - 38 active awards: Phase I, 9 Phase II, 4 Phase II extensions, 2 STTR in 31 topics
- FY 2010
 - 5 new cyber topics approved ; 21 new projects
 - 59 active awards: 21 Phase I, 26 Phase II, 7 Phase II extensions, 5 STTR in 31 topics
- 2007 – present
 - 165 Phase I awards
 - 111 Phase II awards



Summary



- **(U) ASD (R&E) is aligning S&T to realize DoD's strategic vision for operating in cyberspace**
- **(U) DoD Cyber PSC S&T Roadmap sets the direction for future technology investments**
- **(U) DoD Priority Steering Council/Communities of Interest are the coordination mechanism for research and linkage to policy, requirements and operational communities**
- **Increased S&T collaboration across community is evident**



SBIR Website



<http://dodsbir.net/>

All SBIR Proposals must be prepared and submitted electronically through the DoD SBIR/STTR Electronic Submission Web Site <http://www.dodsbir.net/submission/>, as described in Sections 3.0 and 6.0 of the program solicitation.

Future Solicitation Schedule

	Pre-Release	Open	Closed
SBIR Solicitation 2012.1	November 9, 2011	December 12, 2011	January 11, 2012
STTR Solicitation 2012.A	January 26, 2012	February 27, 2012	March 28, 2012
SBIR Solicitation 2012.2	April 24, 2012	May 24, 2012	June 27, 2012
SBIR Solicitation 2012.3	July 26, 2012	August 27, 2012	September 26, 2012
STTR Solicitation 2012.B	July 26, 2012	August 27, 2012	September 26, 2012



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