

UNCLASSIFIED



Cyber PSC S&T Roadmap

26 November 2012

Cyber Priorities Steering Council

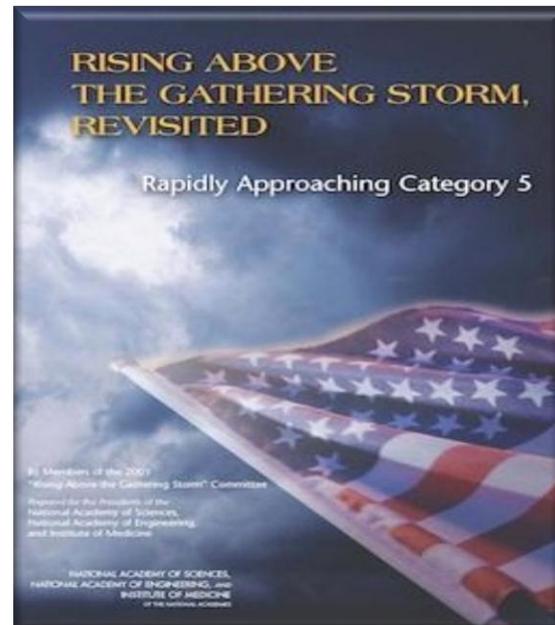
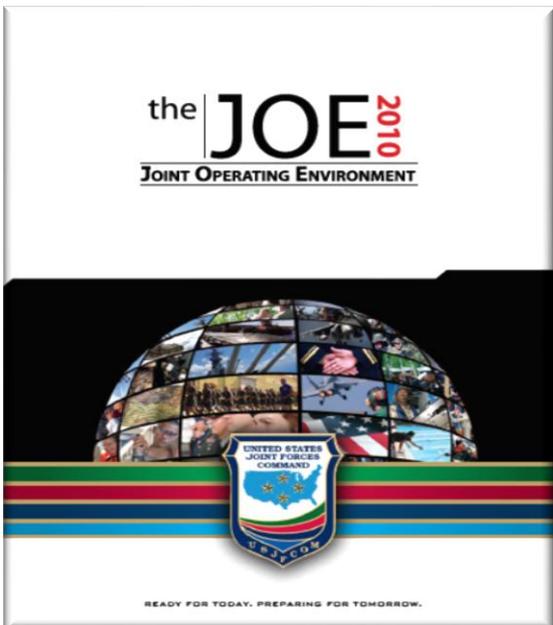
DISTRIBUTION STATEMENT A. Approved for public release; distribution is unlimited

UNCLASSIFIED



UNCLASSIFIED

Global Shifts Drive Global Challenges



Shift in World Demographics
Technology Globalization
Shifting Global Economics
Limited World Energy Resources
Challenges to Existing State Structures
WMD proliferation

Innovation & Competitiveness
Knowledge Capital
Human Capital
Creative "Ecosystem"

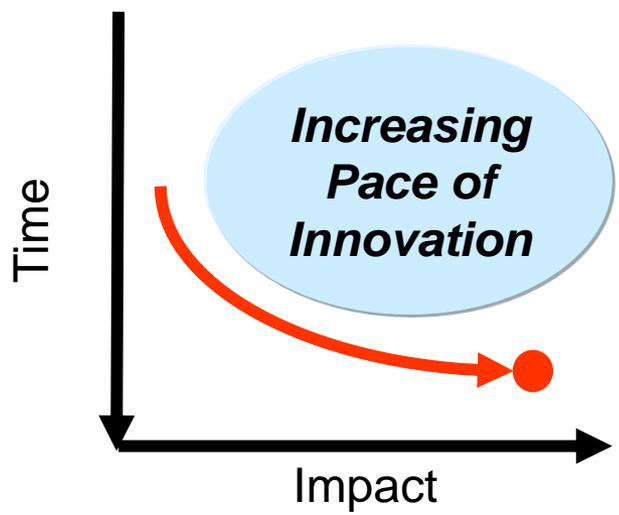
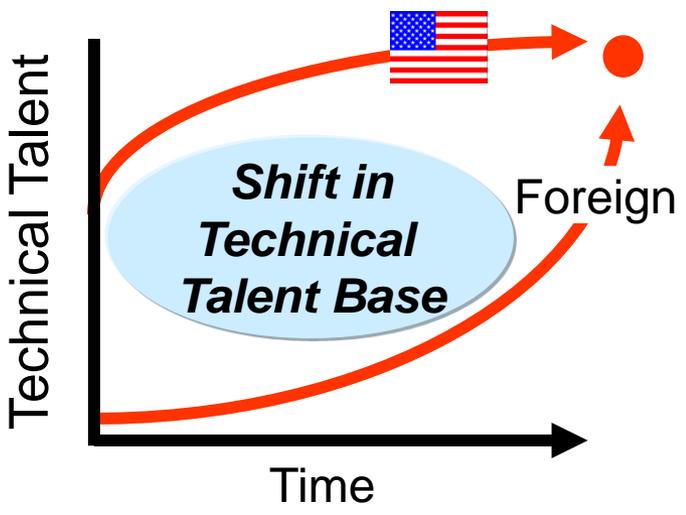
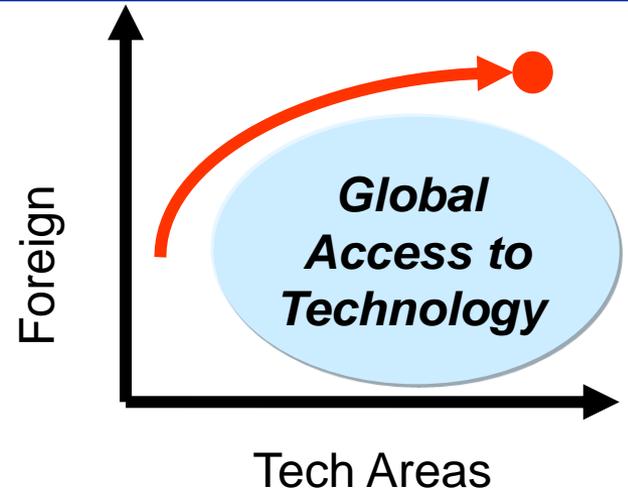
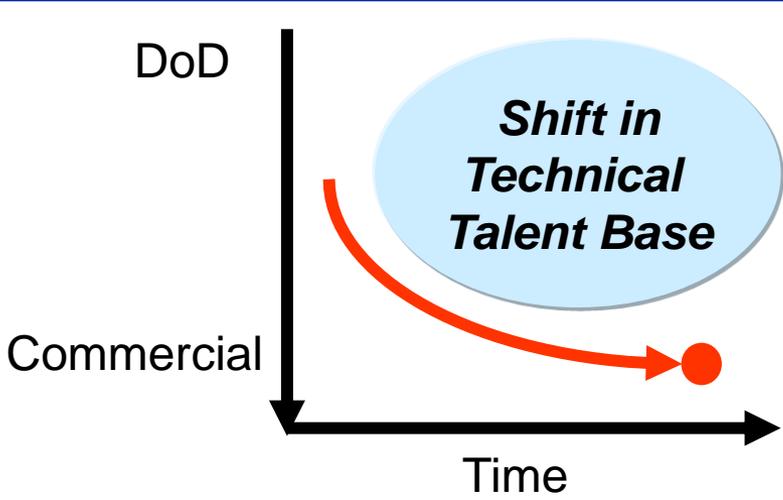
UNCLASSIFIED



UNCLASSIFIED



Key Challenges to our Technical Base



UNCLASSIFIED



UNCLASSIFIED

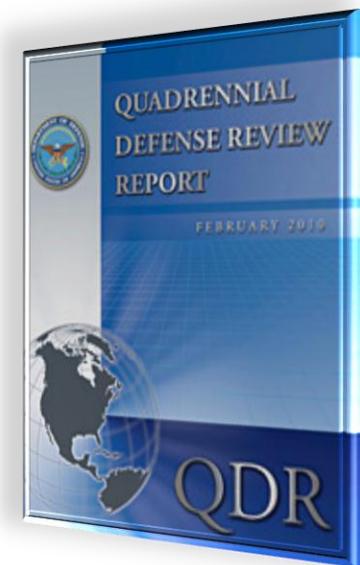


QDR-DPPG Studies

QDR 2010 Key Mission Areas

QDR identified 6 Key Mission Areas that DoD should build capability capacity to be successful in the future global security environment

- Defend the United States and Support Civil Authorities at Home
- Succeed in Counterinsurgency, Stability, and Counterterrorist Operations
- Build the Security Capacity of Partner States
- Deter and Defeat Aggression in Anti-Access Environments
- Prevent Proliferation and Counter Weapons of Mass Destruction
- Operate Effectively in Cyberspace



Studies focused on identifying enabling technologies for capabilities needed in their Key Mission Area

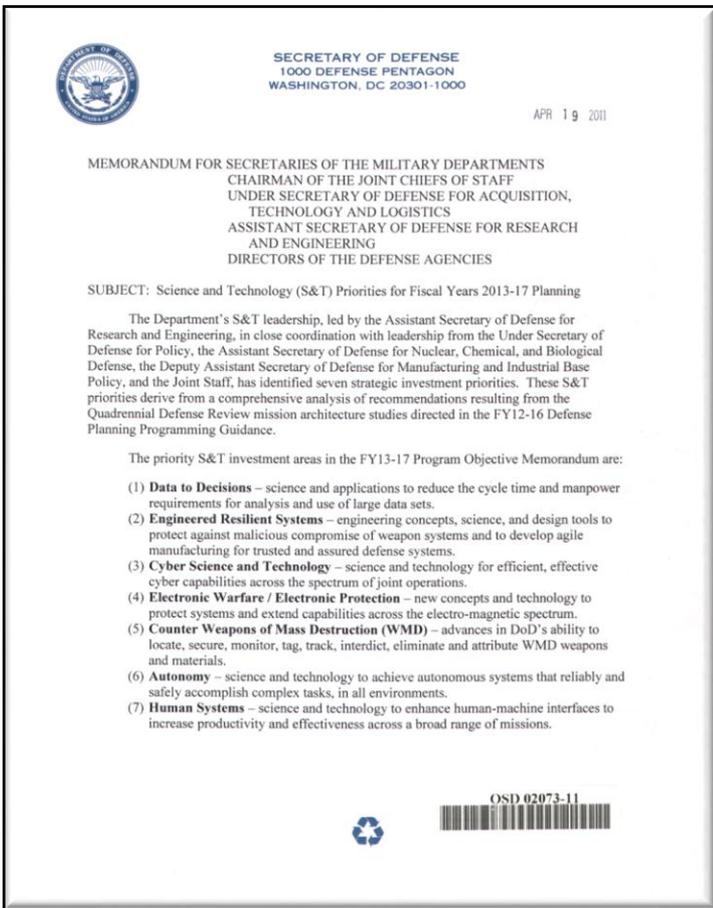
UNCLASSIFIED



DoD S&T Priorities

SECDEF Guidance

Complex Threats



Electronic Warfare / Electronic Protection

Cyber Science and Technology

Counter Weapons of Mass Destruction

Force Multipliers

Engineered Resilient Systems

Data-to-Decisions

Human Systems

Autonomy

19 April 2011



UNCLASSIFIED

Defense Strategy for Operating in Cyber Space



Enhance United States National Security & Economic Prosperity

Cyberspace is the new domain of warfare

Need for active defenses

Ensure the safety of critical infrastructure

Collective defense

Keep the technological advantage

Resiliency

Agility

Mission Assurance

Foundations of Trust

Foundational DoD S&T Thrusts

“Our success in cyberspace depends on a robust public/private partnership. The defense of the military will matter little unless our civilian critical infrastructure is also able to withstand attacks.” ~ Bill Lynn

UNCLASSIFIED



UNCLASSIFIED

Sustaining U.S. Global Leadership: Priorities for 21st Century Defense



SUSTAINING U.S.
GLOBAL LEADERSHIP:
PRIORITIES FOR 21ST
CENTURY DEFENSE

Operate Effectively in Cyberspace and Space. DoD will continue to work with domestic and international allies and partners and invest in advanced capabilities to defend its networks, operational capability, and resiliency in cyberspace and space.

DEFENSE BUDGET
PRIORITIES AND CHOICES



JANUARY 2012

Cyber Operations. The strategic guidance highlights the increasing importance of cyber operations. As a result, cyber is one of the few areas in which we actually increased our investments, including in both defensive and offensive capabilities.

UNCLASSIFIED



UNCLASSIFIED



CYBER PSC S&T ROADMAP

UNCLASSIFIED



UNCLASSIFIED



Problem Statement

- **Problem: DoD lacks agile cyber operations and resilient infrastructure to assure military missions**
 - **Cyber systems are increasingly complex, making them more susceptible to cyber attacks and difficult to 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; this limits their operational decision trade space**
 - Commanders currently have limited ability to evaluate and manage operational risk of cyber assets and actions – local decisions can have global impact
 - **Adversaries exploit severe asymmetric advantages in cyberspace**
 - A single vulnerability may enable widespread compromises
 - **Lack of quantitative metrics and measure for cyber inhibits effective investments in the agility of cyber operations and the resiliency of cyber infrastructure**

UNCLASSIFIED



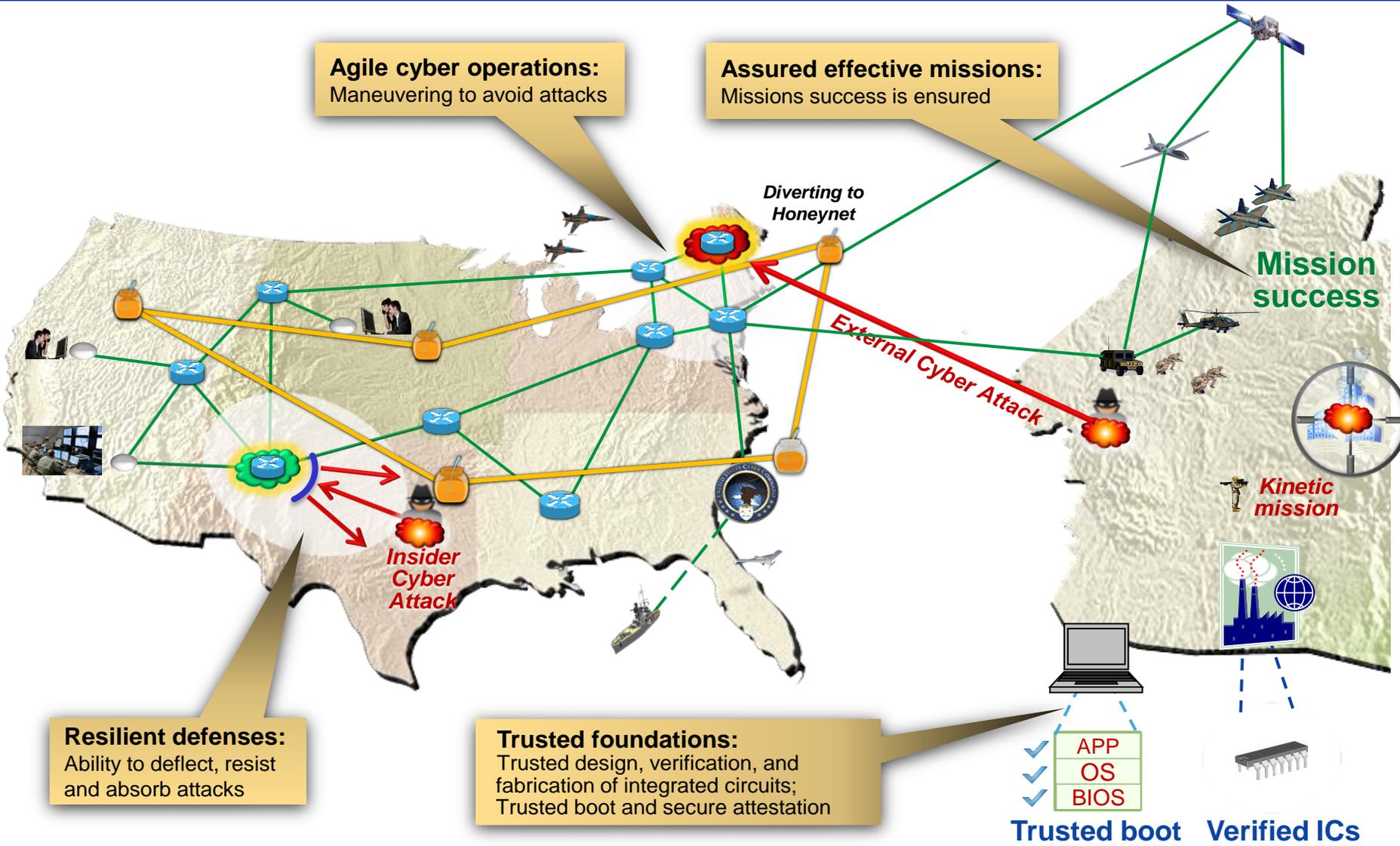
UNCLASSIFIED



Desired End State

Agile cyber operations:
Maneuvering to avoid attacks

Assured effective missions:
Missions success is ensured



Resilient defenses:
Ability to deflect, resist and absorb attacks

Trusted foundations:
Trusted design, verification, and fabrication of integrated circuits;
Trusted boot and secure attestation

UNCLASSIFIED



Cyber Environment

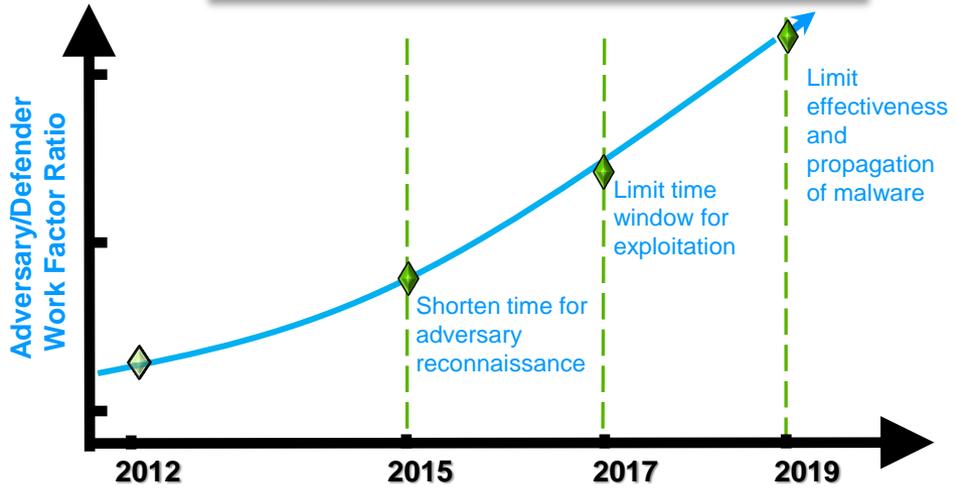
• Missions

- 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



UNCLASSIFIED



Key Capability Areas "4+1"

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 M&S and Experimentation
(Cross Cutter)

UNCLASSIFIED



Priority Gaps Summary

TRUST

- Trusted systems from components of mixed trust

RESILIENCY

- Robust and self-healing cyber infrastructure

AGILITY

- Autonomous responses that occur at net speed
- Tools to enable coordination & control of maneuvers

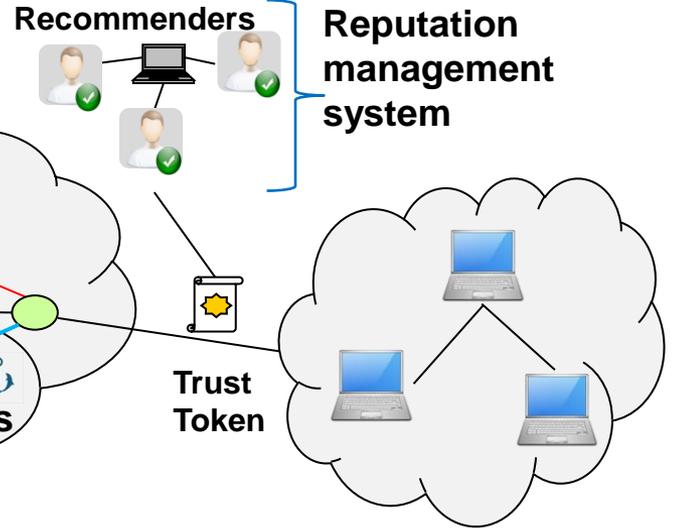
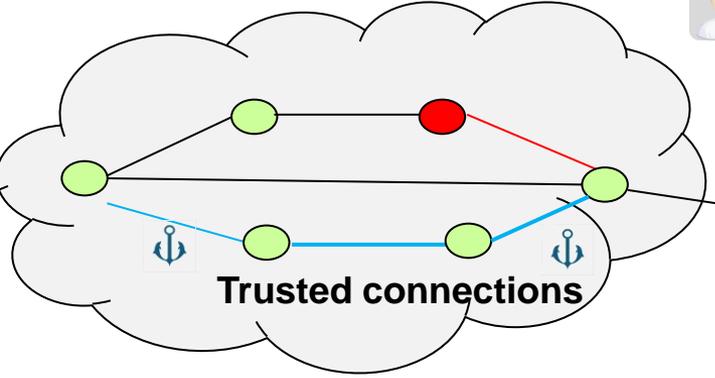
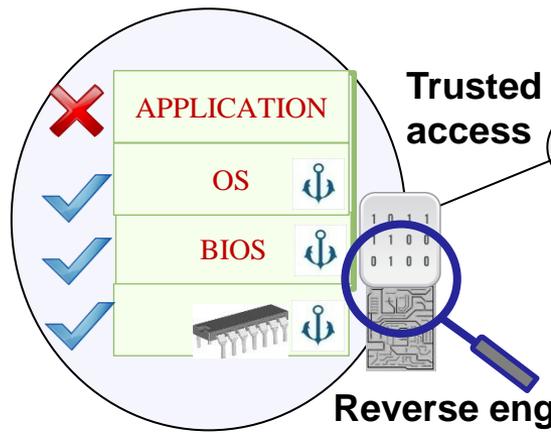
MISSION

- Mission-driven understanding of cyber operations



Key Capability Area: Trust Summary

Trusted boot and operations



Trust Foundations Technology Challenge

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



UNCLASSIFIED



Trust (U)

Tech Challenge: Trust Foundations (U)

(U) Objective: Develop measures of trustworthiness for components within the cyber infrastructure and to large systems where components and participants having varying degrees of trustworthiness

Research Approaches

- **(U) Scalable reverse engineering and analysis**
 - (U) Develop tools that validate and verify hardware chip, firmware and software functionality
 - (U) Develop tools for interoperable and scalable forensic analysis
- **(U) Trust establishment, propagation, and maintenance techniques**
 - (U) Develop techniques to establish trust anchors within components
 - (U) Develop algorithms to describe, establish, propagate, and revoke trust with distributed reputation management
 - (U) Develop algorithms and mechanisms to manage dynamic and transitive trust relations with coalition partners
- **(U) Measurement of trustworthiness**
 - (U) Develop quantitative techniques to enable context-aware dynamic trust scoring of components and systems
 - (U) Develop composite measures of trust
- **(U) Development of trustworthy architectures and trust composition tools**
 - (U) Develop trust architectures that can self attest to their required trust properties
 - (U) Create techniques to build trustworthy systems from untrustworthy components

UNCLASSIFIED

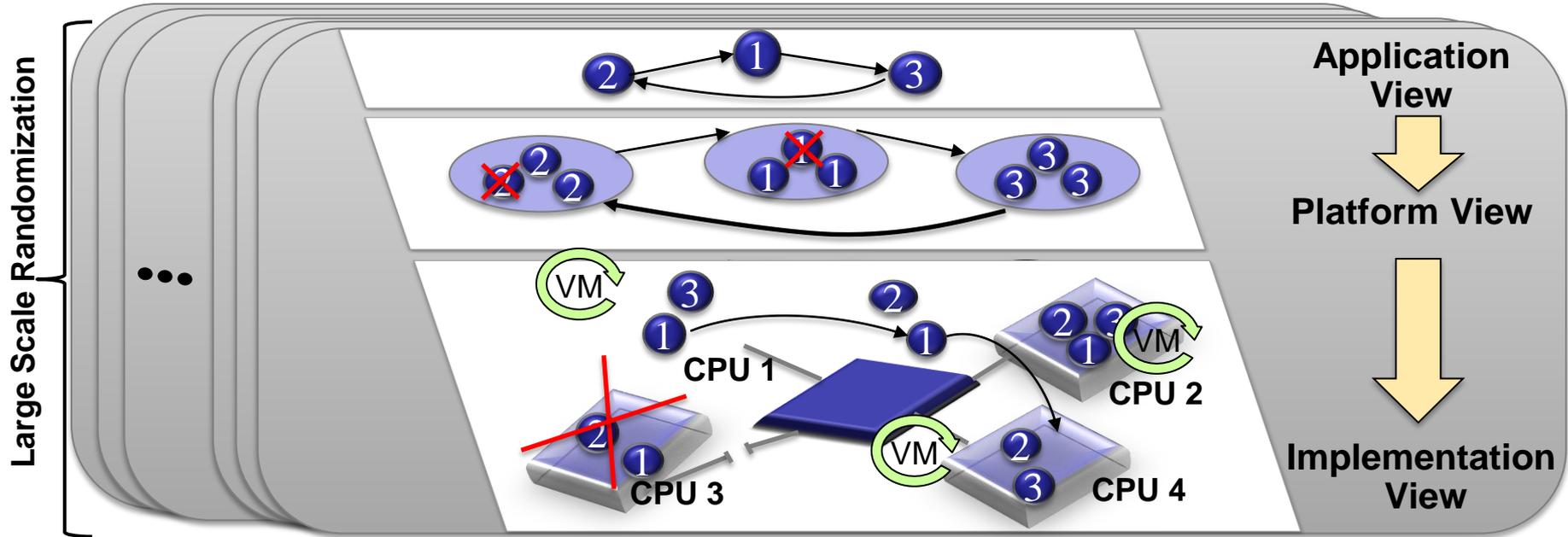


UNCLASSIFIED



Key Capability Area: Resilient Infrastructure

Illustrative Example



Built-in resiliency mechanisms that enable systems to absorb and fight through adversary attacks (e.g., redundancy, diversity, virtualization, randomization, unpredictability, dynamic refresh)

UNCLASSIFIED



Resilient Infrastructures (U)

Tech Challenge: Resilient Architectures (U)

(U) Objective: Develop integrated architectures that are optimized for the ability to absorb shock and the speed of recovery to a known secure state

- **(U) Resiliency for operational systems**
 - (U) Develop efficiency-, risk-, and cost-based approaches to manage real-time tradeoffs among redundancy, randomization, diversity, and other resiliency mechanisms
- **(U) Mechanisms to compose resilient systems from brittle components**
 - (U) Develop architectural foundations to compose and manage services in massive environments
 - (U) Develop resiliency-aware abstraction layers that provide dynamic, threat-based component integration
- **(U) Integration of sensing, detection, response, and recovery mechanisms**
 - (U) Develop automated response tools using information correlated across the infrastructure
 - (U) Develop algorithms for management and outcome analysis of resiliency properties of systems
- **(U) Secure modularization and virtualization of nodes and networks**
 - (U) Enable heterogeneity at the hardware, hypervisor, operating system, and application layers
 - (U) Develop robust cloud architectures to resist intrusions of potentially hostile elements
 - (U) Develop algorithms for real-time reconstitution based on dynamic feedback of macro-level resilience and health
- **(U) Resiliency-specific modeling and simulation techniques**
 - (U) Enable the measurement and analysis of systems' quantifiable resiliency properties

Research Approaches



Resilient Infrastructures (U)

Tech Challenge: Resilient Algorithms and Protocols (U)

(U) Objective: Develop novel protocols and algorithms to increase the repertoire of resiliency mechanisms available to the architecture

Research Approaches

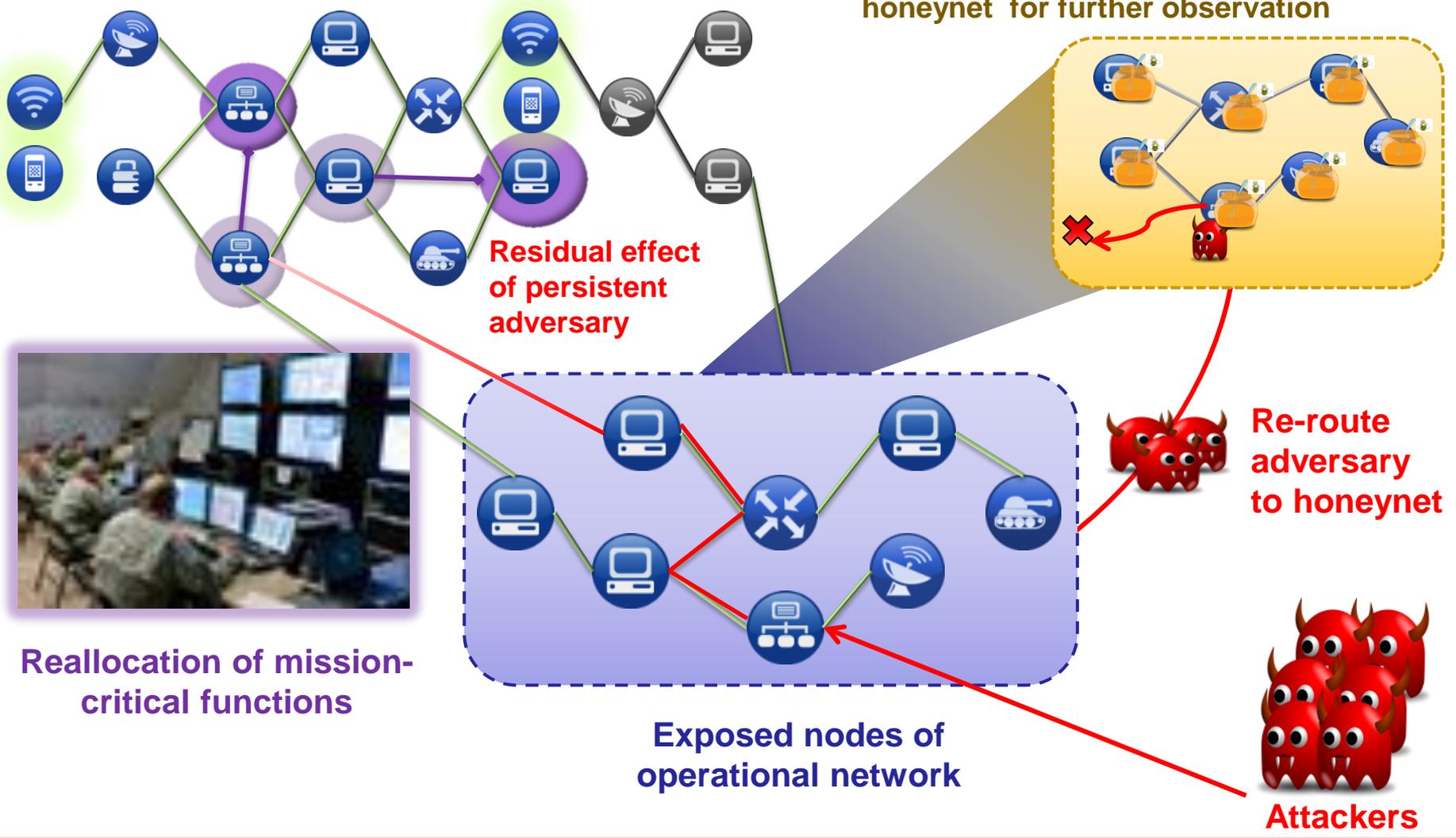
- **(U) Code-level software resiliency**
 - (U) Develop novel language features, randomizing compilation techniques, and enhanced execution environments
- **(U) Network overlays and virtualization**
 - (U) Expedite resilient protocol development using overlays from specification to deployment
 - (U) Develop network reconstitution techniques based on modular design and component virtualization
- **(U) Network management algorithms**
 - (U) Develop autonomous network management algorithms for scalable reconfiguration and self-healing modeled after biological systems
- **(U) Mobile computing security**
 - (U) Develop protection models, mechanisms, and algorithms for mobile devices to ensure higher levels of trust



UNCLASSIFIED



Key Capability Area: Agile Operations Illustrative Example



UNCLASSIFIED



UNCLASSIFIED



Agile Operations (U)

Tech Challenge: Cyber Maneuver (U)

(U) Objective: Develop mechanisms that enable dynamically changing cyber assets to be marshaled and directed toward an objective – to create or maintain a defensive or operational advantage

Research Approaches

- **(U) Distributed systems architectures and service application polymorphism**
 - (U) Develop methods for dynamic provisioning, reallocation, reconfiguration, and relocation of cyber assets at both the system and application layers
- **(U) Network composition based on graph theory**
 - (U) Develop network technologies at the architectural level to enable near real-time reconfiguration
 - (U) Develop algorithms to enable sequenced network reconfiguration actions orchestrated across time and space
- **(U) Distributed collaboration and social network theory**
 - (U) Develop collaborative tools to support near real-time distributed maneuver
 - (U) Realize social networks that incorporate coalition partners' offensive and defensive capabilities

UNCLASSIFIED



UNCLASSIFIED



Agile Operations (U)

Tech Challenge: Autonomic Cyber Agility (U)

(U) Objective: Speed the ability to reconfigure, heal, optimize, and protect cyber mechanisms via automated sensing and control processes

Research Approaches

- **(U) Techniques for autonomous reprogramming, reconfiguration, and control of cyber components**
 - *(U) Develop approaches for autonomous policy-driven reconfiguration using ontologies and control loops*
- **(U) Machine intelligence and automated reasoning techniques for executing course of action**
 - *(U) Develop time-constrained automated control loops that select and execute actions within a goal-seeking framework*

UNCLASSIFIED



UNCLASSIFIED

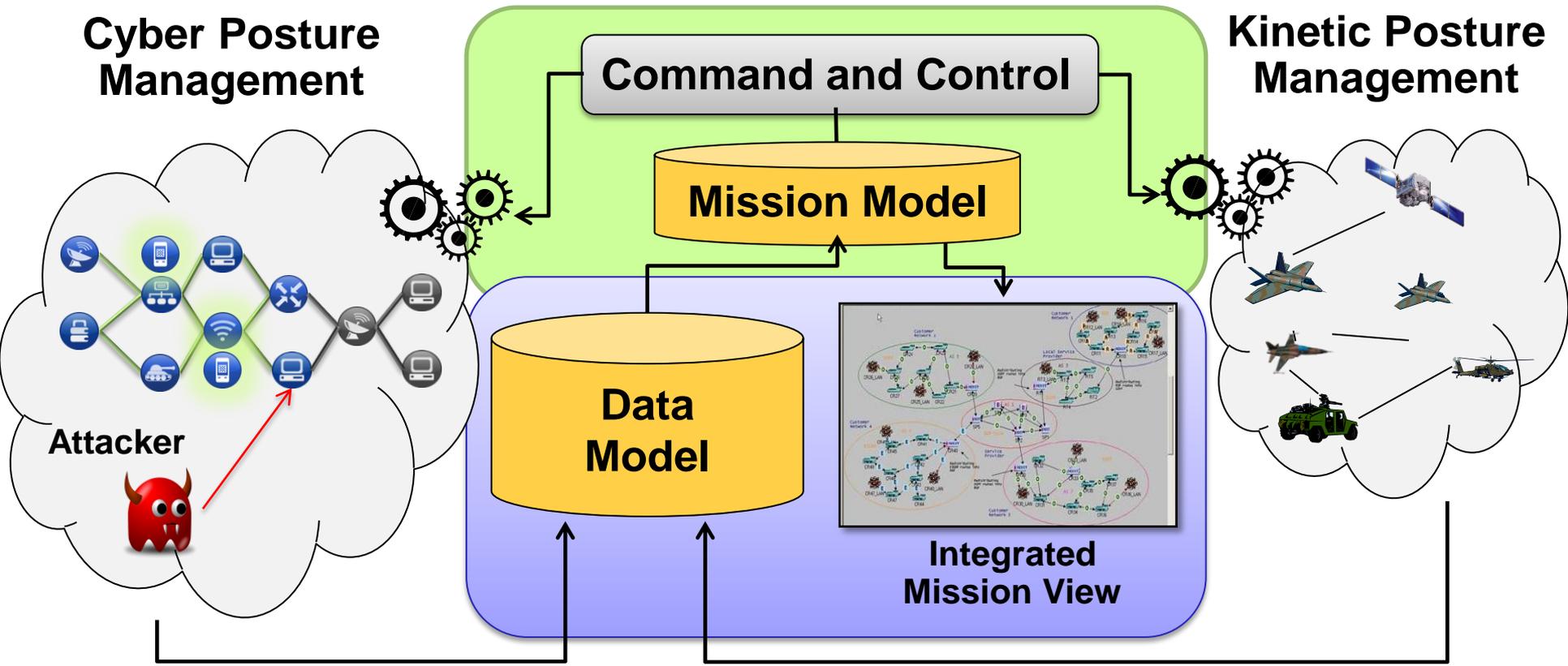


Assuring Effective Missions Illustrative Example

Mission Management

Cyber Posture Management

Kinetic Posture Management



Mission Situational Awareness

UNCLASSIFIED



UNCLASSIFIED



Assuring Effective Missions (U)

Tech Challenge: Cyber Mission Control (U)

(U) Objective: Develop tools and techniques that enable efficient models of blue, grey, and red behavior (cyber and kinetic) to determine the correct course of action in the cyber domain

- **(U) Techniques for mapping assets and describing dependencies between mission elements and cyber infrastructure**
 - *(U) Develop sensors, specification languages, and machine learning for near real-time cyber situational awareness*
 - *(U) Design static and dynamic models and supporting languages that relate cyber and kinetic domains*
 - *(U) Develop near real-time mission analysis tools to support combined cyber/kinetic operations*
- **(U) Techniques for course-of-action analysis and development**
 - *(U) Develop modeling and simulation techniques for assessment of asset criticality and effects*
 - *(U) Design game-theoretic approaches to predict adversarial behavior*
 - *(U) Develop tools for mission simulation, rehearsal, and execution support*
- **(U) Cyber effects assessment**
 - *(U) Develop probing, detection, correlation, and visualization techniques*

Research Approaches

UNCLASSIFIED



Cyber Modeling & Simulation, and Experimentation/Range Technology

- **Sound, Integrated Experimentation is Needed to Accelerate Progress and Prove Value**
 - Within and Across PSC Theme Areas
 - Over All Aspects of Cyber Operations, in Context of Mission
 - Well-Defined Metrics, Realistic Scale
 - Both Scientific and Exercise-Style
- **Cyber Measurement Campaign Plan Development is Underway**
 - Identified Experiments as Proofs of Concept
 - Analyzed Gaps and Needed Experimentation Facilities
 - Described Plan For Developing Enhanced Experimentation Capabilities
- **Future Cyber Modeling and Simulation Campaign Launch Expected in 2013**
 - Early and often assessment of promising cyber operations capabilities.

Cyber “Empire Challenge” Vision

- **Co-organized by the Cyber S&T PSC and USCYBERCOM**
- **Conducted Annually or Biennially – Organized Around a Well-Detailed Mission Thread**
- **Planning Occurring Over the Course of a 6-month Period**
- **Demonstration of Emerging PSC Roadmap Capabilities Coming from:**
 - Service Labs
 - NSA R2
 - DARPA
 - Industry

Bring Operational and S&T Communities Together to:

- Expose New Capabilities to the Operational Community
 - Work Out Early Issues Related to CONOPS and TTPs
- Refine Requirements for S&T Community
- Identify Opportunities for Rapid Fielding



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

METRICS for:

- Resilient Infrastructure
- Trust
- Operational Agility
- Assuring Effective missions

- **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.

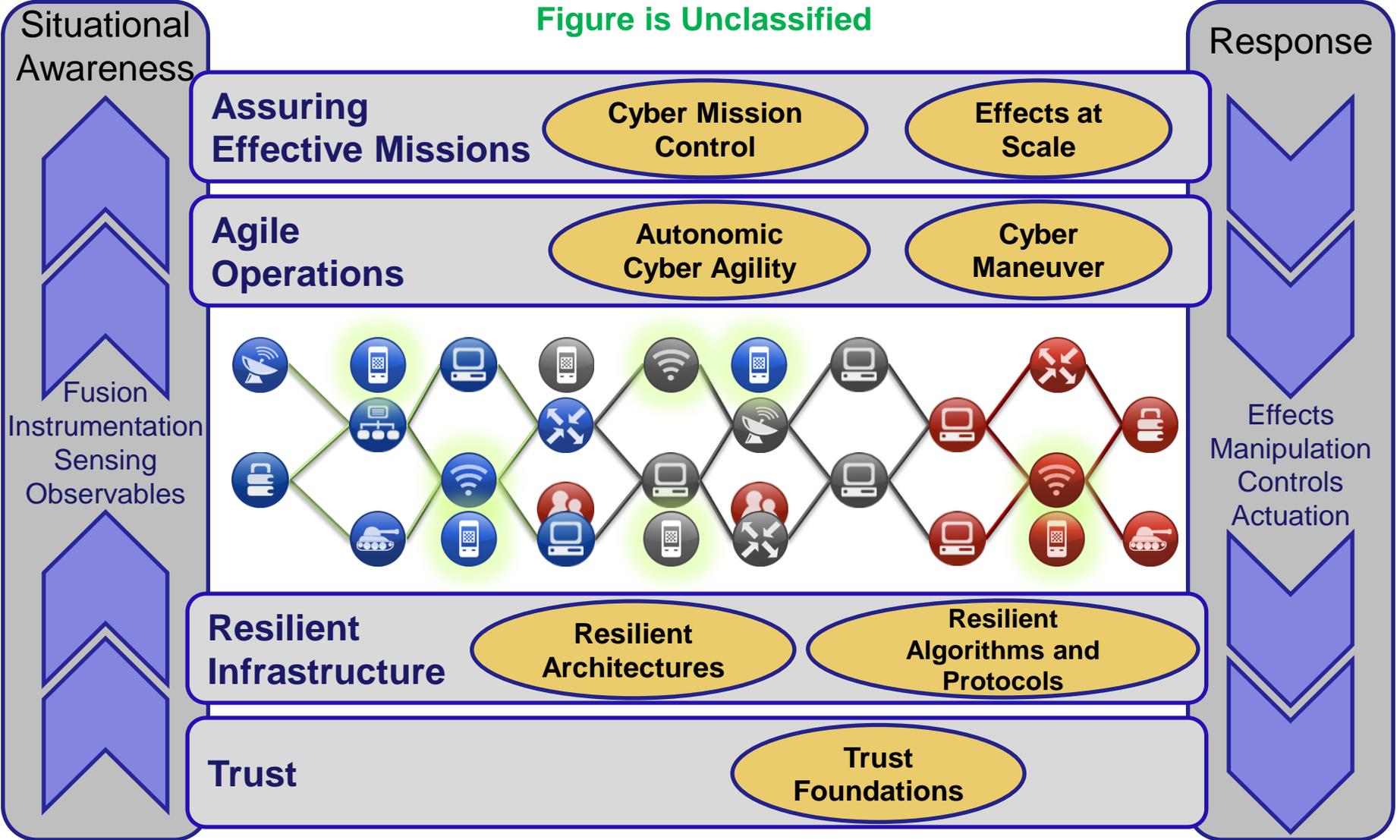


UNCLASSIFIED



Technology Challenge Summary

Figure is Unclassified



UNCLASSIFIED



UNCLASSIFIED

Open Broad Agency Announcements (Updated as of 15 Nov 12)



- **Army Research Office (ARO)**
 - Solicitation #:W911NF-12-R-0012; BAA for Basic and Applied Research, Research Area 5
- **Army Research Laboratory (ARL)**
 - Solicitation #:W911NF-12-R-0011; BAA for Basic and Applied Research, Core Competency 3
- **Communications and Electronics Research, Development, and Engineering Center (CERDEC)**
 - Solicitation #: W15P7T-08-R-P415
- **Office of Naval Research (ONR)**
 - Solicitation #: ONRBAA 13-001, Code 31 Section 1
- **Naval Research Laboratory (NRL)**
 - Solicitation #: BAA-N00173-02, Section 55-11-01 (Information Management and Decision Architectures)
 - Solicitation #: BAA-N00173-02, Section 55-11-02 (Mathematical Foundations of Computing)
 - Solicitation #: BAA-N00173-02, Section 55-11-03 (High Assurance Engineering and Computing)
 - Solicitation #: BAA-N00173-02, Section 55-11-04 (Advanced Naval Network Solutions)
 - Solicitation #: BAA-N00173-02, Section 55-11-05 (Adversarial Modeling and Decision Support)
 - Solicitation #: BAA-N00173-02, Section 55-11-06 (Software Engineering for High Assurance Computer Systems)
- **Air Force Office of Scientific Research (AFOSR)**
 - Solicitation #: AFOSR-BAA-2012-0001, Section c.
- **Air Force Research Laboratory (AFRL)**
 - Solicitation #: BAA-10-09-RIKA (Cross Domain Innovative Technologies)
 - Solicitation #: BAA-11-01-RIKA (Cyber Assurance Technologies)
- **Defense Advanced Research Projects Agency (DARPA)**
 - Solicitation #: DARPA-BAA-12-29 (Research topics of interest to the I2O office)

**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

UNCLASSIFIED



UNCLASSIFIED



BACK-UP

- INCLUDE CYBER M&S / EXPERIMENTATION FROM SIPR SLIDES
- UPDATE BAA LISTING

UNCLASSIFIED



Problem Statement Theme Areas 10 Year Objectives

Vision

10 Year Objective

Assuring Effective Missions	Can track infrastructure state and cyber attacks, understand and predict how they affect mission functions	<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>
Agile Operations	Infrastructure allows systems and missions to be reshaped nimbly to meet tactical goals or environment changes	<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>
Resilient Infrastructure	Missions are difficult to disrupt even with successful cyber attack	<ul style="list-style-type: none"> <i>Autonomous self-managing resilient systems</i> <i>Mobile devices with fully attested hardware, firmware, and applications</i>
Trust	Quantitative trust in systems as built and in operation; systems of known trust from elements of mixed trust	<ul style="list-style-type: none"> <i>Trusted systems from components of mixed trust</i>