Cyber Science and Technology
OSD and the Military Services
27 November 2012

Steven King, Ph.D.
Office of the Assistant Secretary of Defense, Research and Engineering (R&E)

S&T Influencing the DOD Cyber Landscape

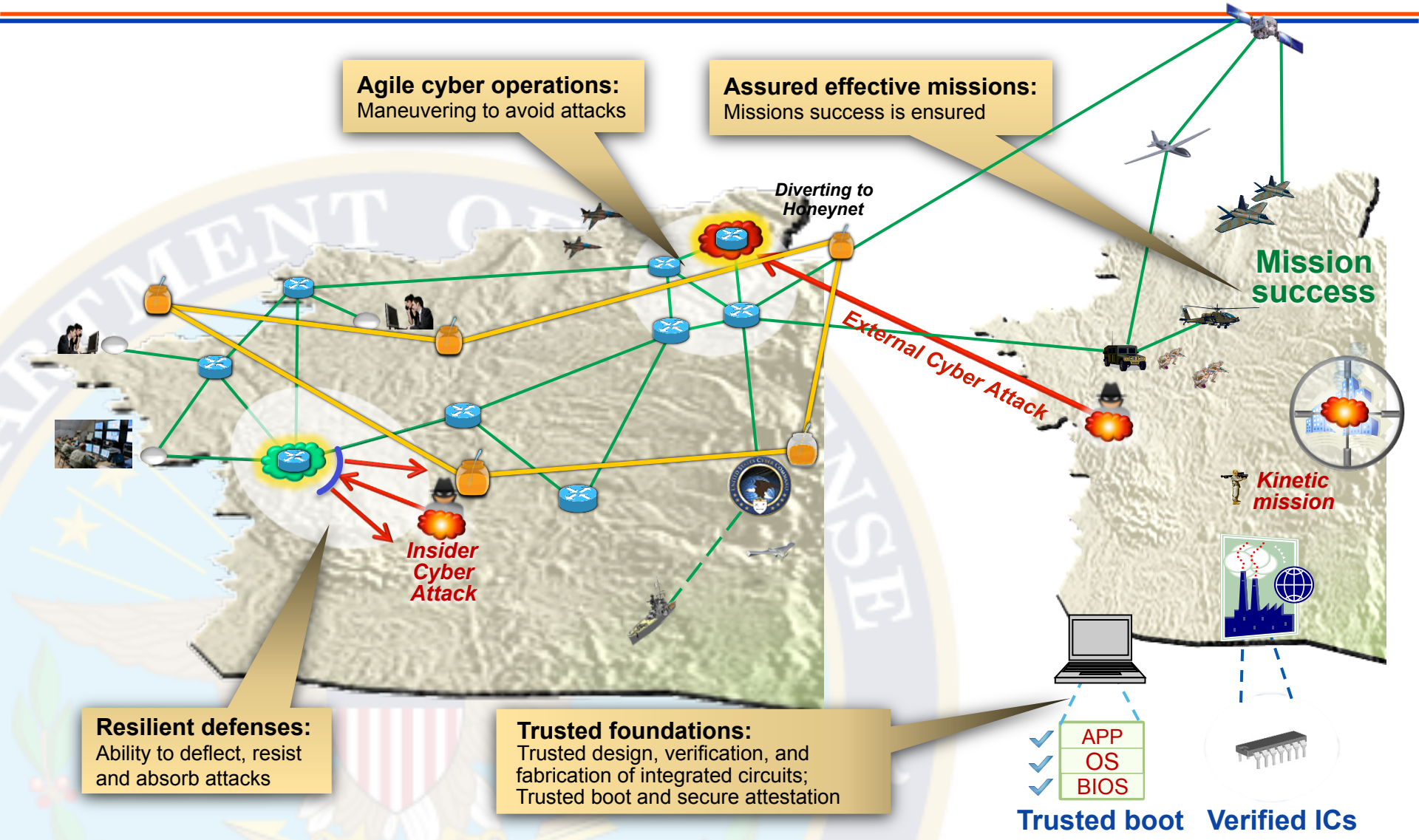
" Our success in cyberspace depends on a robust public/private partnership. The defense of the military will matter little unless our civilian critical infrastructure is also able to withstand attacks." ~ Bill Lynn

Cyber Integration Group (CIG)

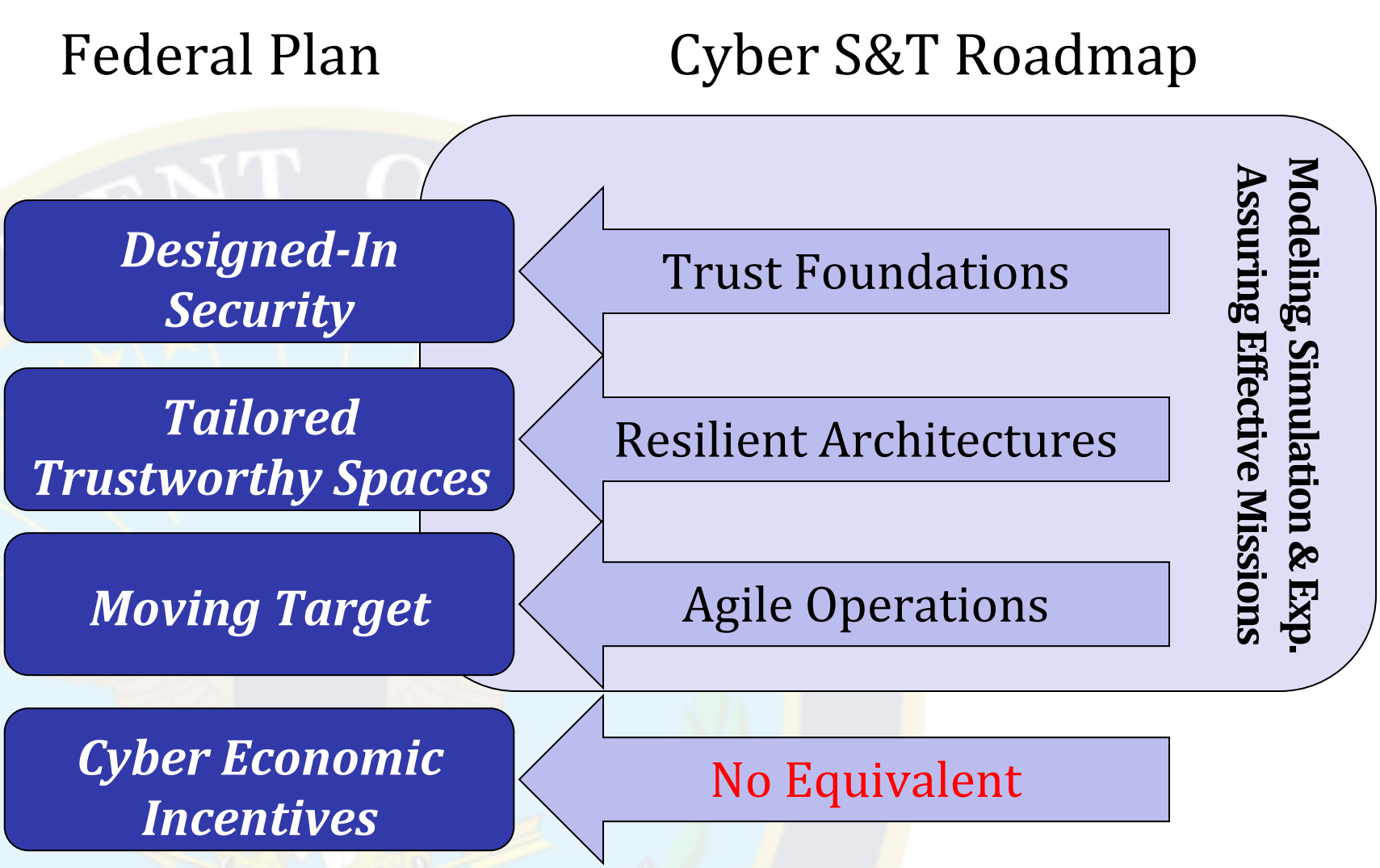
Cyber Investment Management Board (CIMB)

COCOMs

Research Roadmap
Problem Statement



Themes to Gaps



University Outreach

- **Multidisciplinary University Research Initiatives (MURI)**
  - Maintains efforts in basic research in areas of DoD interest
  - Engages and utilizes academic sector in DoD priorities
  - 16 ongoing projects, $19 Million in FY 2011
  - Large scale university collaborations (~$1.0 M/year for 5 years)

Basic Research Examples

- **AFOSR – Dr. Robert Herklotz, robert.herklotz@afosr.af.mil**
  - Science of cyber security MURI
    - Advance the science base for trustworthiness by developing concepts, relationships, and laws with predictive value.
  - Individual PI awards on securing network, hardware, data, and human/ computer elements of security
- **ONR – Dr. Sukarno Mertoguno, sukarno.mertoguno@navy.mil**
  - Strengthen research on future need toward secure, predictable and more efficient software
  - Network/node high-speed hardware/firmware modeling, simulation and emulation
  - Research on fundamental components for autonomic computing
  - Research for automation in cryptology
- **ARO – Dr. Cliff Wang, cliff.x.wang.civ@mail.mil**
  - Hardware assurance
  - Cyber situation awareness
  - Mobile ad hoc wireless communication security and robustness

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)
- **FY11 – today: sponsored 71 SBIR projects focusing on Cyber Research (~$16.2M)**
- **Going forward, SBIR Topics will reflect the goals of the Roadmap**

Foundations of Trust	Agile Operations
Resilient Infrastructure	Assuring Effective Missions

- **Examples of current open topics include:**

AF131-055: End to End Network Trust
AF131-051: Conflicting, Suspicious, and Inconsistent Information Detection (CSI-Info)

For more Information

- **ARL Broad Agency Announcements**

  http://www.arl.army.mil/www/default.cfm?page=8

- **ONR Broad Agency Announcements**

  http://www.onr.navy.mil/en/Contracts-Grants/Funding-Opportunities/Broad-Agency-Announcements.aspx

- **AFOSR Broad Agency Announcements**

  http://www.wpafb.af.mil/library/factsheets/factsheet.asp?id=8127

- **Defense Advanced Research Projects Agency (DARPA)**

  http://www.darpa.mil/

- **DoD Small Business Innovative Research (SBIR)**

  http://dodsbir.net/

- **DoD Cyber S&T Roadmap**

  http://www.acq.osd.mil/chieftechnologist/areas/cyber.html

Backup

NAME: DR. ROBERT HERKLOTZ

BRIEF DESCRIPTION OF PORTFOLIO:

Fund science that will enable the AF and DOD to dominate cyberspace: Science to develop secure information systems for our warfighters and to deny the enemy such systems.

LIST SUB-AREAS IN PORTFOLIO:

1: SOS-Science of Security
2: Secure Humans
3: Secure Networks
4: Secure Hardware
5: Covert Channels
6: Execute on Insecure Systems
7: Secure Data
8: Secure Systems-Security Policy

Science of Cyber Security MURI Goals

- **Scientific objective**
  - Advance the science base for trustworthiness by developing concepts, relationships, and laws with predictive value.
- **Technical approach**
  - *Security modeling:* characterize system, threats, and desired properties. Leverage game-theoretic concepts to model incentives for the defender and attacker.
  - *Composition:* develop principles for explaining when security schemes compose, and how to achieve compositionality.
  - *Security Measurement:* goals include determining relative strengths of defense mechanisms, evaluating design improvements, and calculating whether additional mechanism is warranted based on attacker and defender incentives

Navy FY 2014 Budget Highlights in CSIA

- Basic & Applied Science Research
  - Research on fundamental components for Autonomic Computing
    - Knowledge/model representation and infrastructure for supporting reasoning and system dynamism
    - Symbiotic integration of Machine Learning & Machine Reasoning for supporting self-awareness
  - Research for Automation in Cryptology
    - Enhancing automated cryptographic security proving
    - Automated exploration for cryptographic primitives in various fields.
    - Automated search for secure variants of AES

Navy FY 2014 Budget Highlights in CSIA

- Basic & Applied Science Research
  - Strengthen research on future need toward secure, predictable and more efficient software
    - In (coding) progress, interactive code analysis, abstraction and model generation for enhancing programmers' awareness of their code and for supporting (providing model) for autonomic computing
    - Security and predictability for programs/software in CPS environment
    - Automated post processing for reducing program complexity and improving software security and efficiency.
      - Software development support for effective automated software complexity reduction

Navy FY 2014 Budget Highlights in CSIA

Cyber S&T Development and Assessment Environment

- Network/Node Modeling and Simulation
- Virtual Network and Application Integration
- Large Scale Storage
- High Speed Hardware/Firmware Modeling and Emulation

Information Assurance Program Vision and Research Thrusts

Program Vision

To create the foundations of the science of security and underlying principles of robust and resilient systems that enable the processing and delivery of authentic, secure, reliable, and timely information to warfighters, regardless of threat conditions.

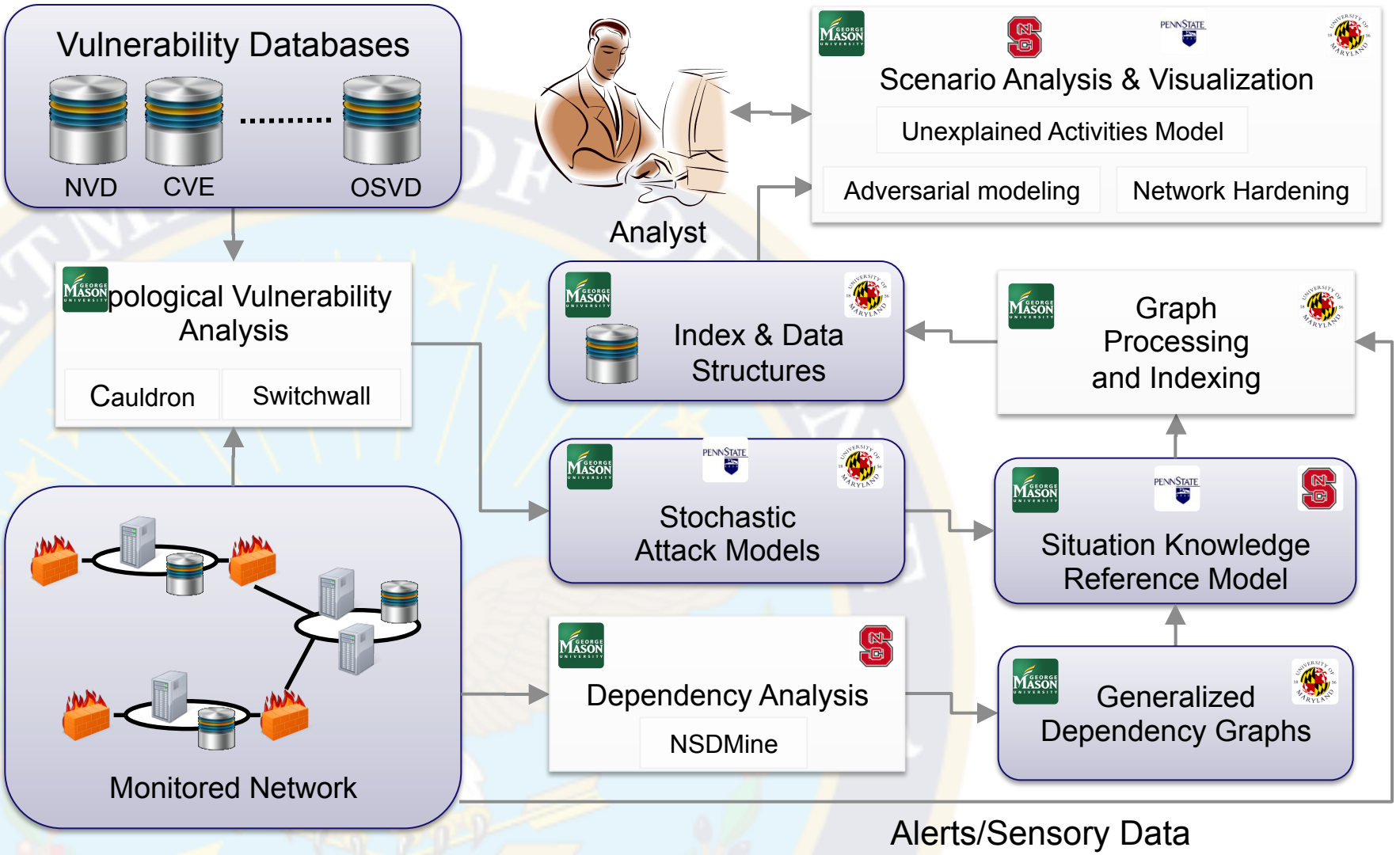
Research Thrusts

- Resilient and Robust Information Systems
- Highly Assured Tactical Information

Focus areas:

- Hardware Assurance
- Cyber Situation Awareness
- Mobile ad hoc Wireless Communication Security and Robustness

Resilient & Robust Information Systems Strategy, Accomplishment and Status



Highly Assured Tactical Information Objectives and Opportunities

Scientific Objectives

- Obtain new scientific understandings of trustworthy tactical communications, especially on physical layer properties for authentication and verification
- Establish fundamental principles and models for robust and resilient tactical information processing that enables a clean slate secure network design
- Develop information assurance metrics in the tactical environment

Scientific Barriers/Challenges to Overcome

- No comprehensive quantification model exist for Wireless ad hoc mobile communication with unpredictable characteristics, even without considering the presence of adversarial attacks.
- No reliable model exists for predicting sudden change of peer relationship or node capturing.

Scientific Opportunities

- New understanding of wireless channel state models and the associated channel signature enables security techniques such as localization
- More holistic understanding on trade-offs between performance and security through cross layer experiments, modeling, and analysis