



Mission Based Analysis for Cyber Measurement and Mission Assurance

*Wende Peters
The Johns Hopkins University
Applied Physics Laboratory
wende.peters@jhuapl.edu*

28 OCT 2009

Agenda

- **NIAEC: Past and Present**
- **IA Best Practices Demonstration**
- **Beyond NIAEC: Cyber Measurement and Mission Assurance**

History: What Is NIAEC?

NIAEC Mission: *Provide a forum for engagement among those who develop and operationally deploy IA solutions to enhance national security by moving IA technologies into the hands of warfighters*

- Insert IA technologies into operational scenarios and realistic system configurations
- Demonstrate the effects and impacts in a realistic OPSIT
- Educate operational users on the abilities and benefits of emerging IA solutions
- Educate IA researchers on operational needs and likely employment scenarios
- Facilitate technology transition from researchers to programs of record



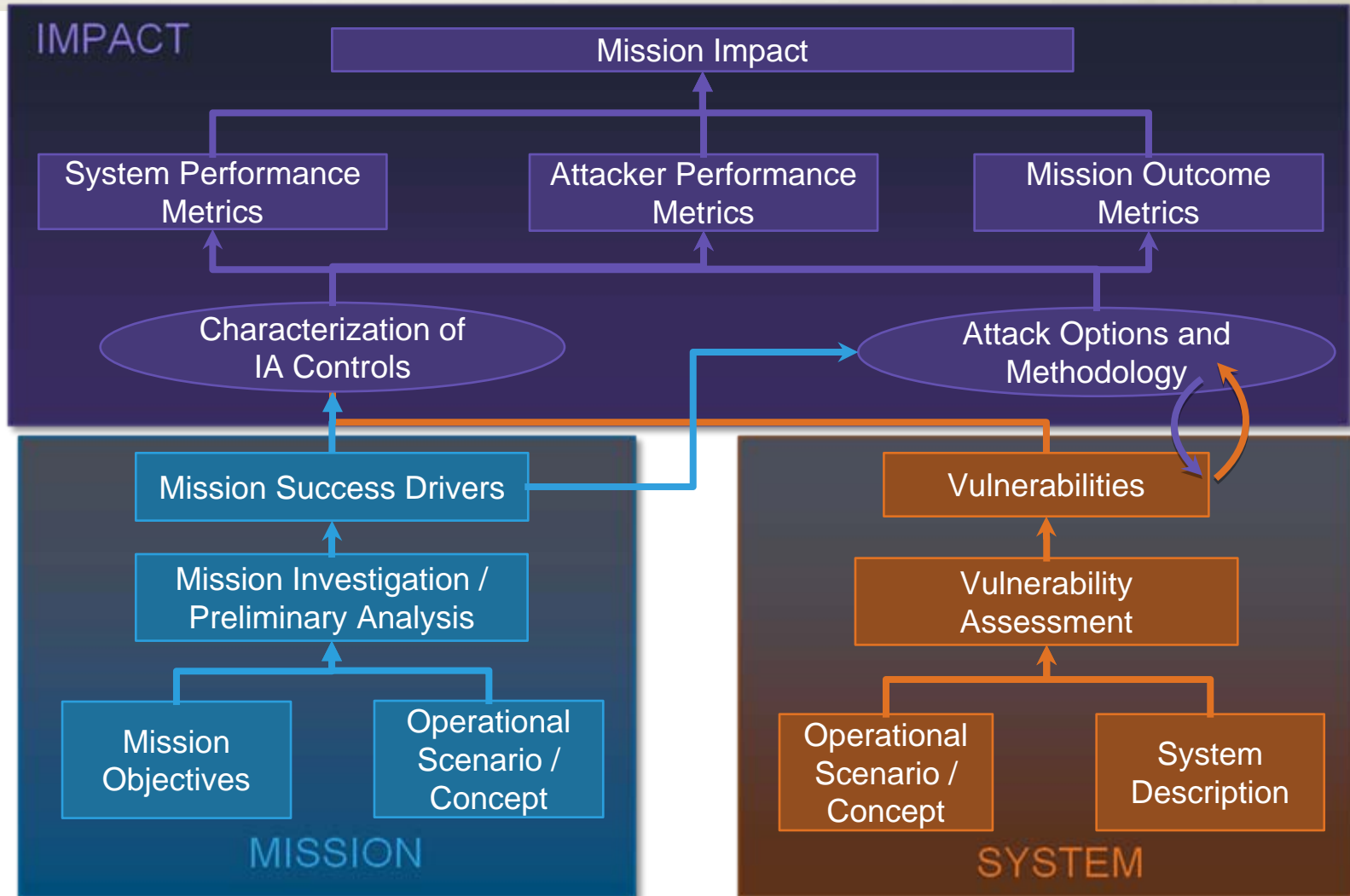
NIAEC 1.0

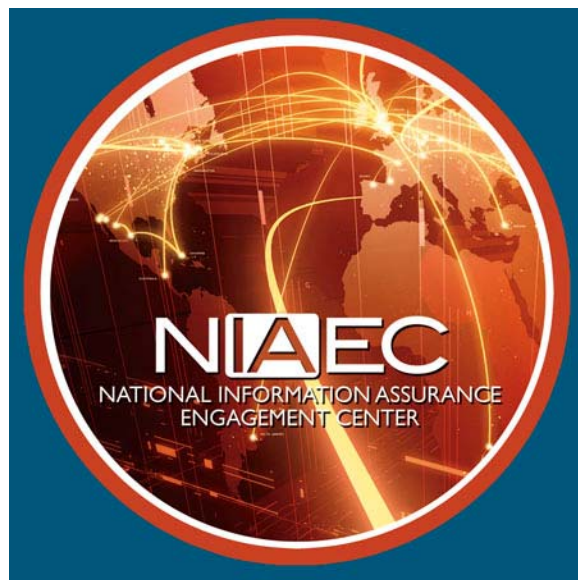


FOCUS: *Awareness*

- *Threat – you are at risk*
- *Technology– there are ways to mitigate*
- *Operations – how real-world employment should drive IA research*

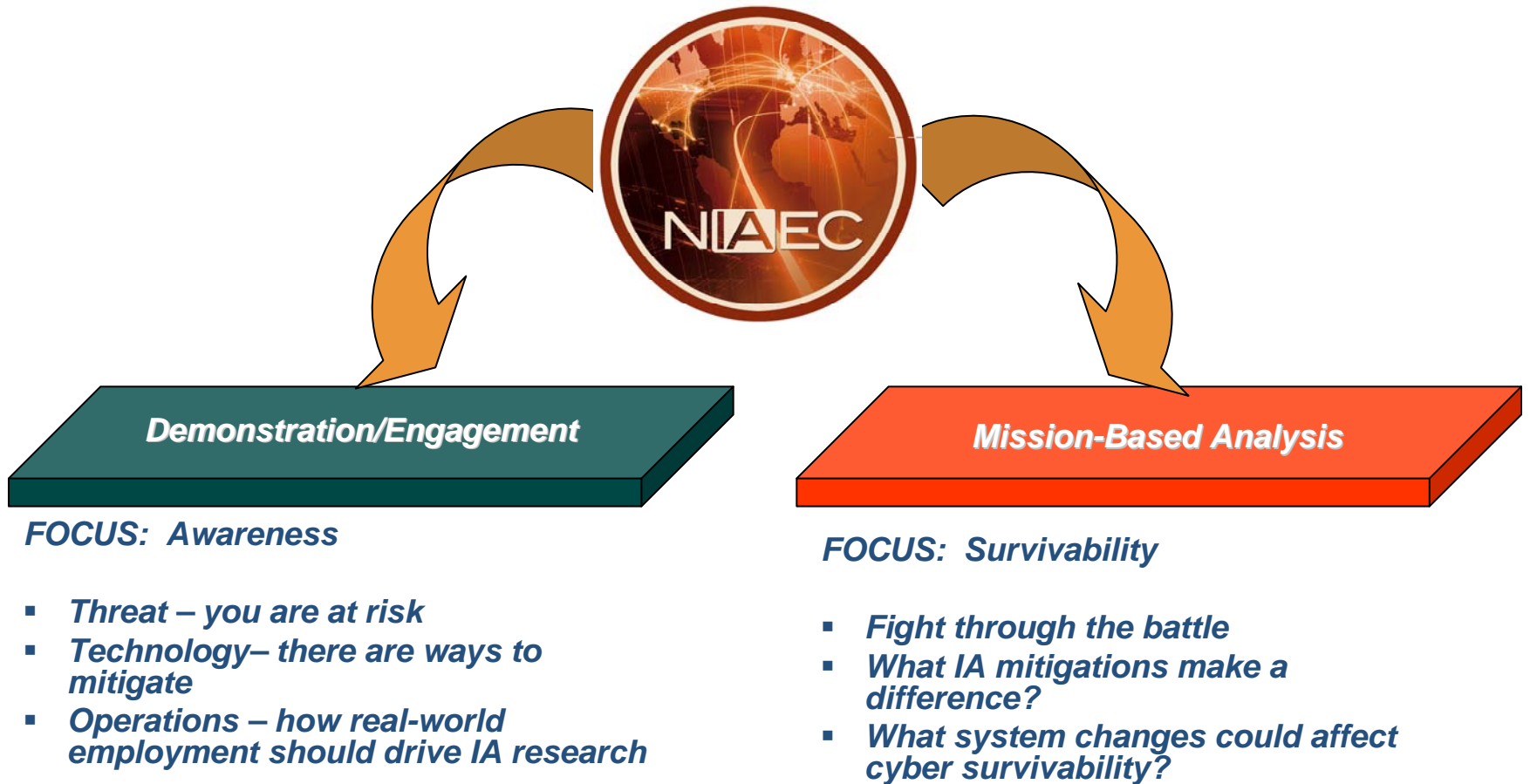
Mission Based Cyber Analysis





NIAEC Demo Excerpt

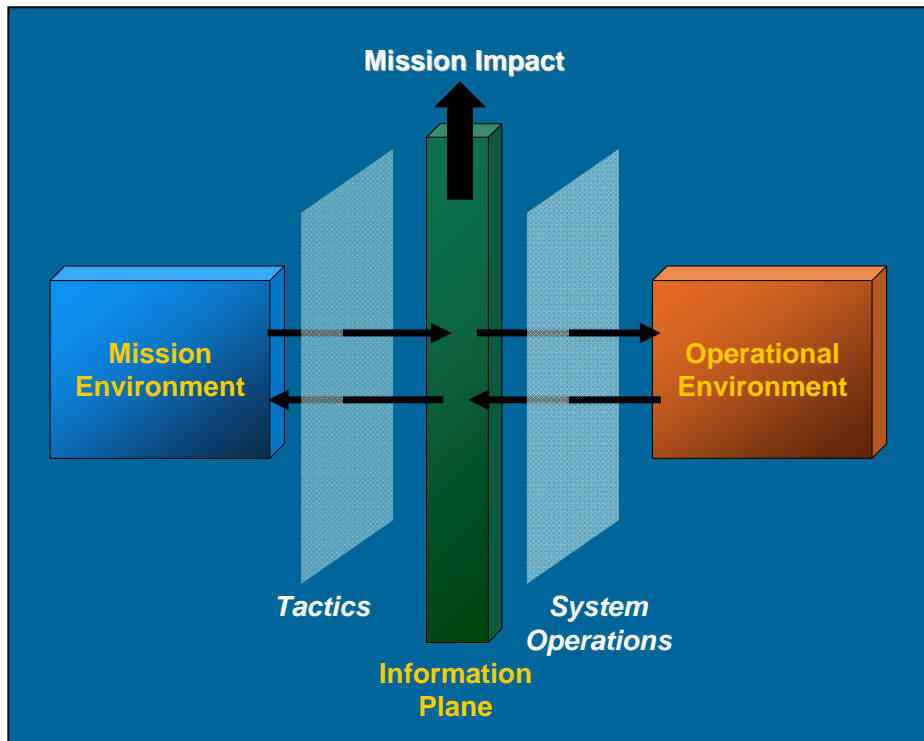
NIAEC 2.0: Expanding Focus to Meet the Challenge



The Challenge

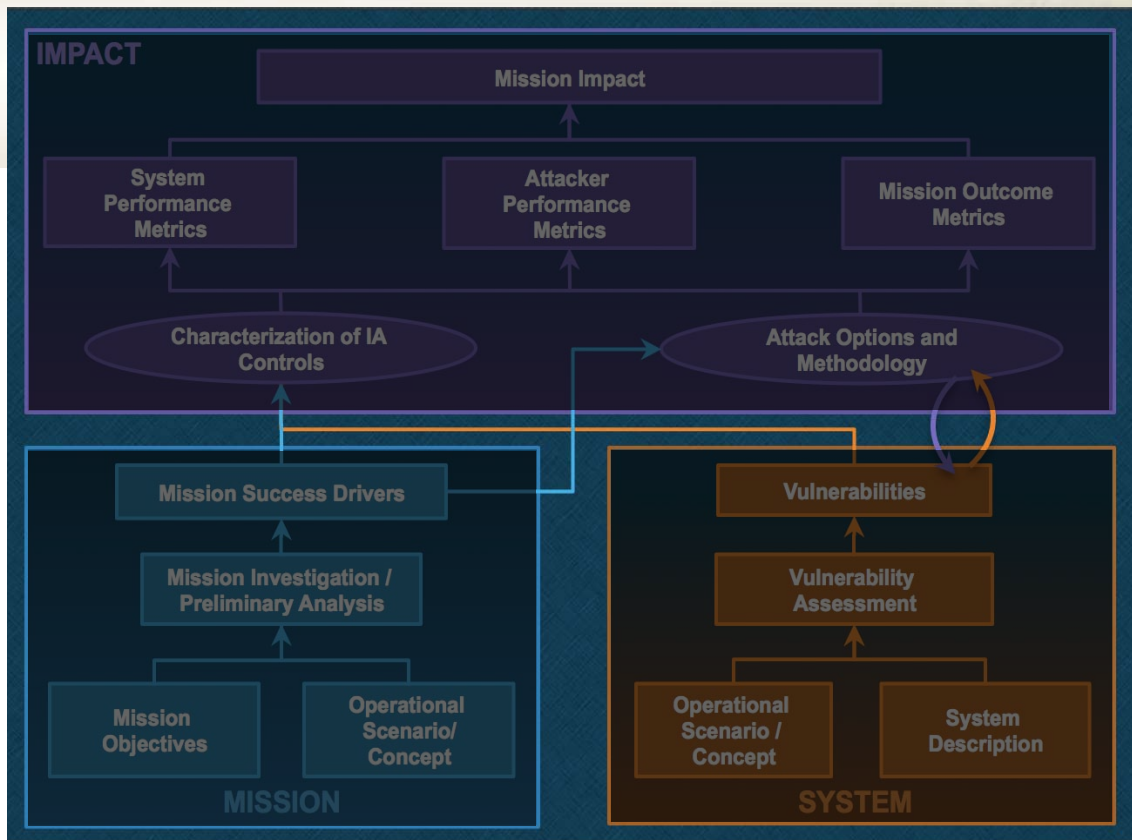
- How do we *measure* the effects of IA investment, system security, cyber activity to allow:
 - Investment decisions and trade offs
 - Assessment of performance
 - Operational soundness
 - Readiness/preparedness
- What makes any of these measurements meaningful?
 - **MISSION – MISSION-MISSION**

Attacking That Challenge



***Our Hypothesis:
Mission outcome can be affected,
determined, or measured via
operations on the information plane***

- Develop the combination of methodologies and approaches that:
 - Represents mission success drivers in terms of information flows
 - That represents system operations in terms of information flows
 - That can be operated on so that changes in system state (via cyber activity) can drive mission outcome
 - That can be operated on so that changes in mission can be correlated to system vulnerabilities



MISSION ANALYSIS QUESTIONS

- How do we express mission consistently to operations on it?
- How do we assign value to decomposition of mission MOEs?
- How do we account for mission variability and non-cyber drivers?

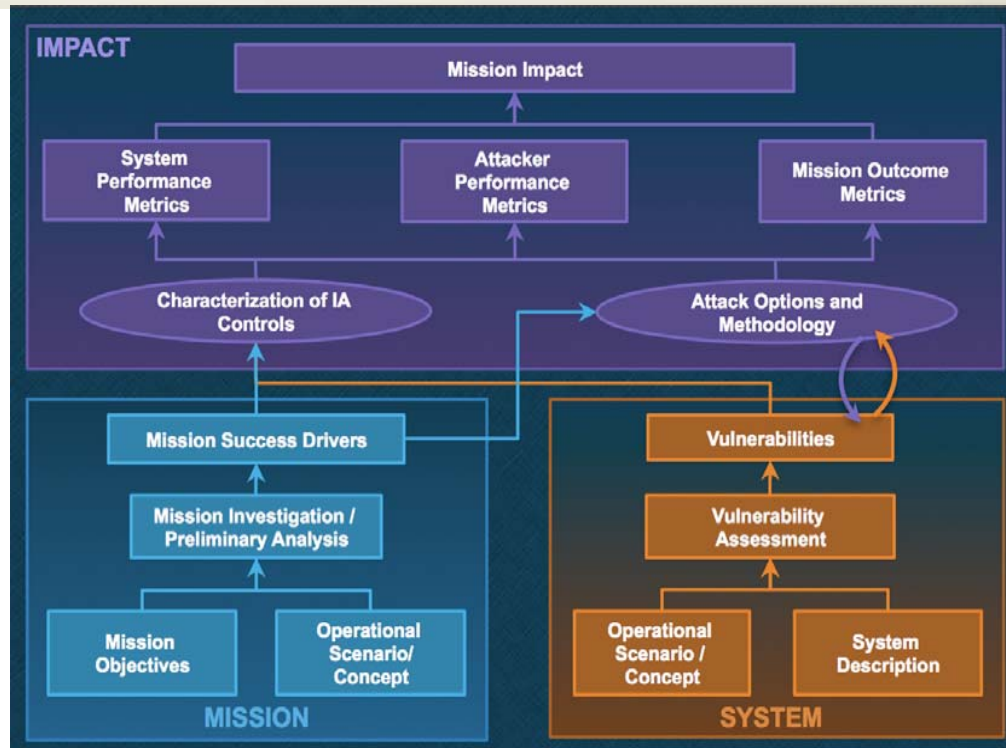
IMPACT ANALYSIS QUESTIONS

- How do we characterize IA controls to operate on the information plane?
- How do we characterize attackers/attack vectors to operate on information plane?
- What variations of IA controls or attacks must be permitted for different mission types?

SYSTEM ANALYSIS QUESTIONS

- How do we characterize system performance for operational systems? As-spec'd systems? Projected system capabilities?
- How do we incorporate disparate cyber and non-cyber (network, physics-based) models for cyber analysis?

The REAL Hard Problems



INTEGRATION SCALABILITY OPERABILITY

Looking Forward

- **NIAEC continues to operate in its role of Education, Awareness, and Technology Understanding**
- **Tackling the cyber measurement and mission assurance challenges requires cooperative effort across community**
 - **Best of breed needs to be brought together**
 - **Expansion of model types and approaches**
- **NIAEC looking to connect with COIs and researchers to bring the mission capabilities to bear**
 - **Opportunities to ‘mash up’ our solutions on common scenarios**
 - **Align with NIAEC visitors and obtain feedback on operational needs**

niaec@jhuapl.edu