



Cyber Challenges for Space Systems*

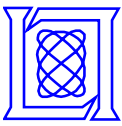
PRESENTED AT THE
GSAW 2010 Workshop

J. W. Haines

3 March 2010

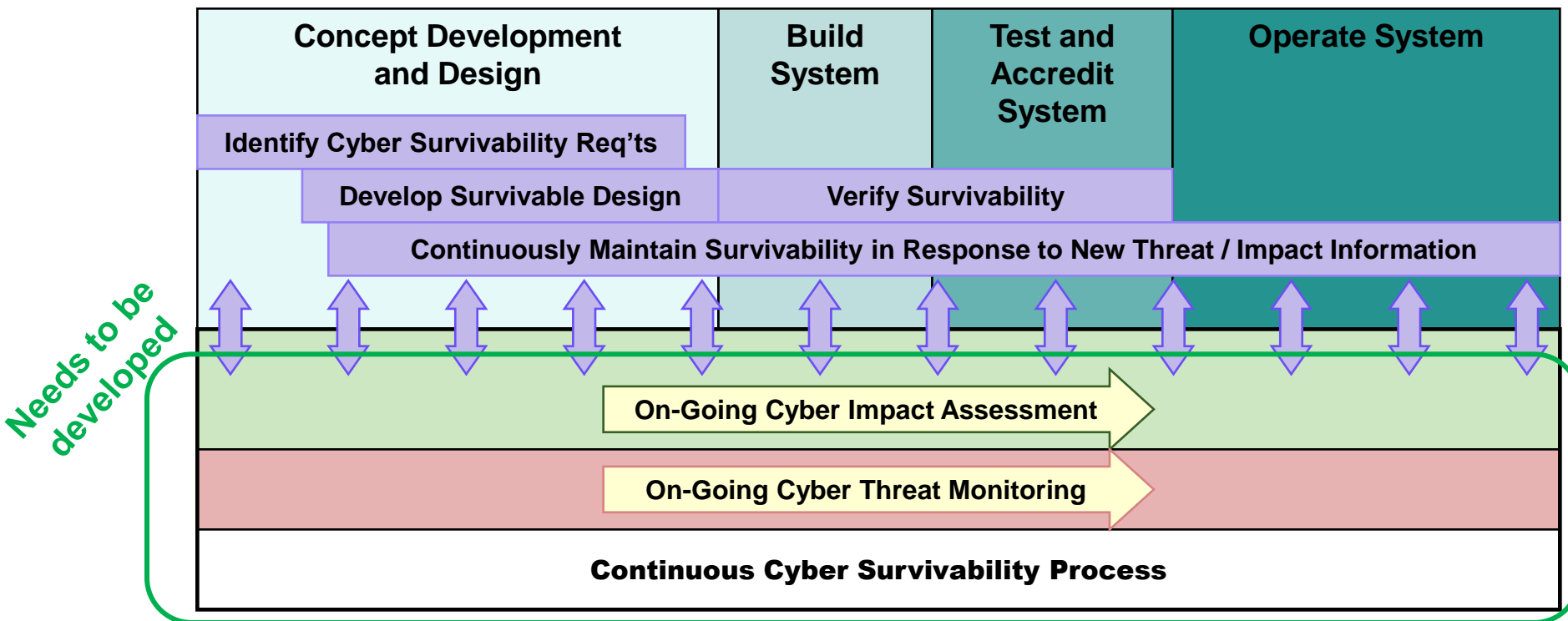
MIT Lincoln Laboratory

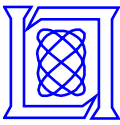
* This work is sponsored by the Department of Defense under Air Force Contract FA8721-05-C-0002. Opinions, interpretations, conclusions, and recommendations are those of the authors and are not necessarily endorsed by the United States Government.



The Vision: Acquiring Cyber Survivable Systems

- **Cyber Survivability:** The ability of a system to withstand a specified level of cyber attack while continuing to provide a specified level of mission function
- Approach should be on-going, repeatable and evolvable to:
 - Enable system architects and designers to design for cyber threat
 - Enable program office to show how well their system will work in the face of each threat
 - Ensure cyber survivability is incorporated in each phase of the system life cycle

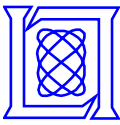




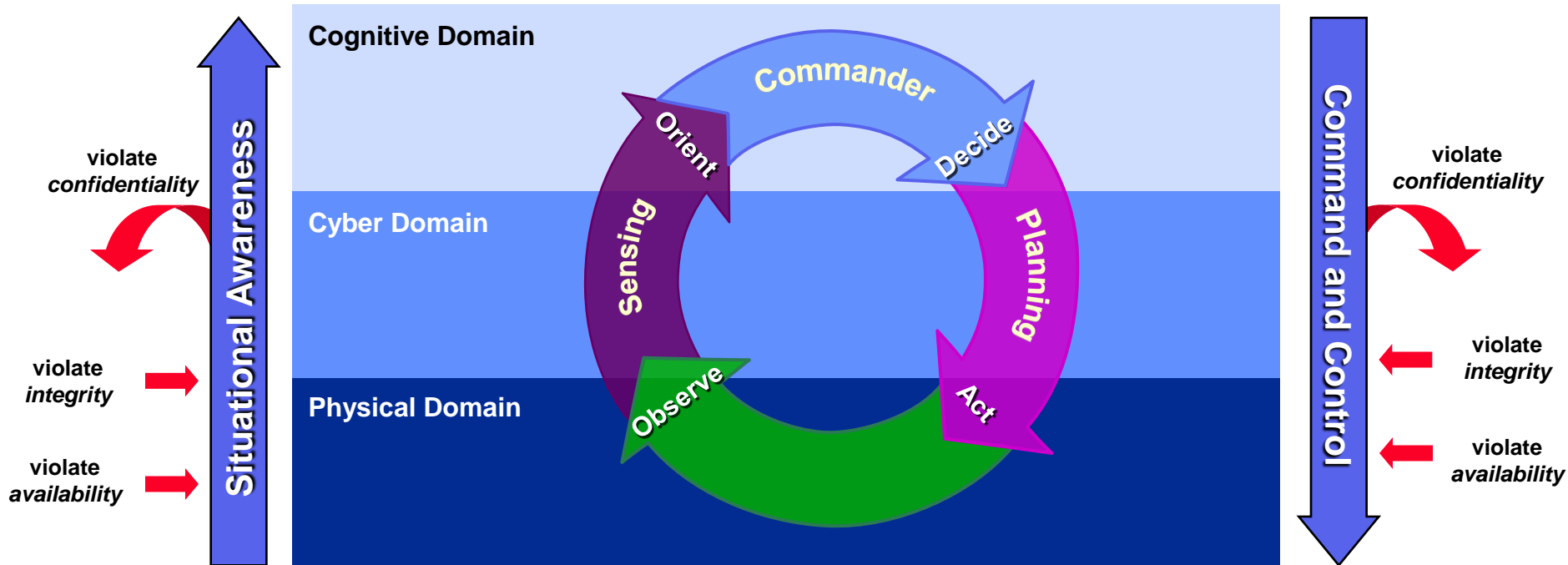
Dynamic Aspects of Security

- **People will make mistakes and attackers will get in (by our mistakes or otherwise)**
- **Model cyber security with a control loop**
 - To get ahead, we must execute our OODA loop more quickly than the adversary
- **Current weaknesses are two-fold**
 - Adversary is not sufficiently resource-constrained
 - We often get stuck in the Orient step
- **Structure information environment to aid in executing our dynamic processes and hinder adversarial processes**





Cyber and the Space Domain



Adapted from Air Force Doctrine Document 2-5, 11 January 2005, adapted from Understanding Information Age Warfare (D.S. Alberts)

- **Concern that adversary may launch coordinated cyber/kinetic attack**
- **Cyber security: integrity, availability, and confidentiality**
- **Cyber services framework**
 - Provides cyber survivability (mission operates through cyber attack)
 - Facilitates cyber countermeasures



Cyber C2 Services

Example of SOA-Based Cyber Battle Manager

Cyber Services

Cyber Alert



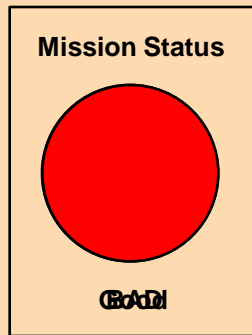
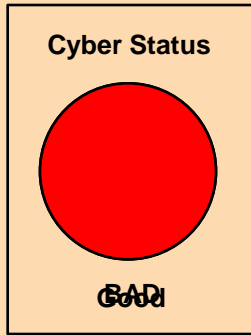
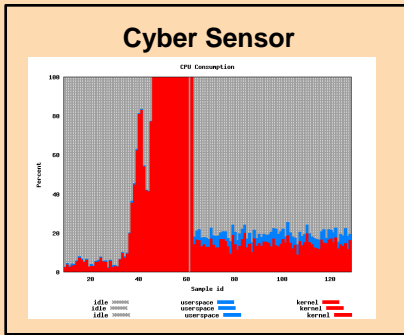
Cyber Network Status



Cyber Mission Alert



Cyber Response



Cyber Situational Awareness Processing Chain

Cyber Alert

Cyber Network Status

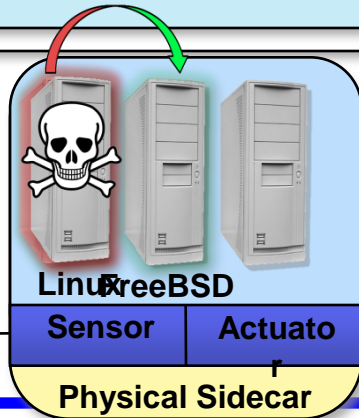
Cyber Mission Alert

BMD Battle Manager

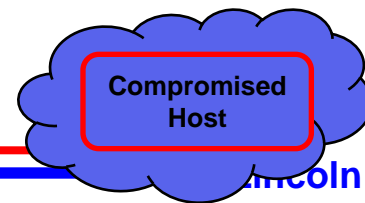
Cyber Response



TRADEX



Linux-specific DOS



Compromised Host



Engineering Cyber Survivable Systems – The Larger Picture

Cyber Assessment

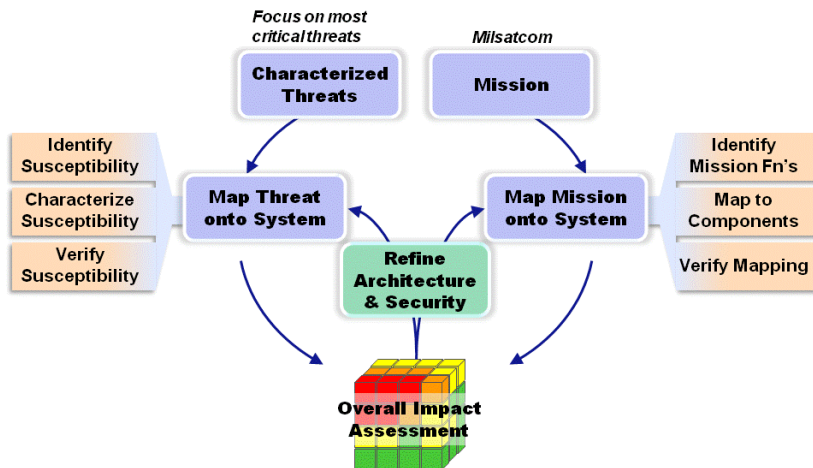
- Understanding the current and potential future threats
- Understanding the system and mission
- Understanding risk to mission from threats

Survivable System and Architecture Development

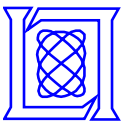
- Applying cyber defense techniques
- Applying fault tolerance and resiliency techniques

Technology Development and Rapid Prototyping

- Prototyping assessment tools
- Prototyping architecture frameworks and interfaces
- Prototyping components of survivable system



SMC and MCSW will need these capabilities for operation of current systems and development of future systems



Cyber Survivability for Space Systems

Bringing it All Together

- **POLICY:** Develop and implement a SMC-wide policy for Cyber Survivability
 - The policy should define Cyber Survivability, set high-level expectations for SMC systems, and assign organizational responsibility for the activities necessary to achieve and verify Cyber Survivability
- **CAPABILITIES:** Cyber domain equivalents of several existing activities & capabilities will need to be initiated:
 - Threat identification, mission impact evaluation
 - Development of technical and architectural mitigations
 - Development of technology, tools, and best practices
- **INTEGRATION:** Integrate Cyber Survivability into all phases of the acquisition process
 - This should include requirements generation, development, deployment, and operations. The mitigation of Cyber threats will likely require a development tail that persists for the operational life of the system

Main Engineering Roles, Tailor specifically for space systems