



U.S. Army Research, Development and Engineering Command



TECHNOLOGY DRIVEN. WARFIGHTER FOCUSED.

Cyber Security Applied Research &
Experimentation Partner BAA

Mr. William Glodek, (A) Network Security Branch Chief
18FEB 2013



ARL's Cyber Security Vision



- Cyber Security is critical to Army's missions
 - Increasing reliance on information technology and communication
 - Information and Communications must be assured, protected, defended
 - Situational Awareness (right info, right place, right time)
- Operational Environments
 - Tactical
 - Strategic
 - Locally and Abroad
- Difficult to Protect & Assure
 - Expansive and complex threat surface
 - Technology Convergence
 - Variety of adversaries
 - Multiple threats

Military



Communications

- Hybrid networks: Convergence of mobile ad hoc, cellular, fixed
- Resource constrained, dynamic
- High & multiple levels of security
- Coalition interoperability



Information

- Search noisy, volatile, incomplete, untrustworthy, hidden, adversarial
- Discovery of hidden attributes, semantic links, structures needed
- Analytics of heterogeneous, noisy, dynamic, & adversarial nets



Social-Cognitive

- Growing use of highly dynamic social networking
- Potential subversion of network, challenged trust
- Evolving, adversarial, social structures, influences, attitudes

Increased complexity of design, discovery, prediction, & control
Increased interactions between comms, information, & social networks



Advance the State of the Art in Cyber Security



- Research and Innovative Experimentation
 - Develop fundamental scientific understanding
 - Focus on specific Research Areas
 - Human effects (Cross Cutting Research Initiative)
- Two-pronged Approach
 - Cyber Security CRA
 - Basic Research (6.1)
 - Theories and Models (mathematically formulated)
 - Produce experimentally testable predictions
 - Cyber Security AR&EP
 - Applied Research (6.2)
 - Perform experimental validation
 - Provide feedback to CRA Researchers
 - Basic Research (6.1)
 - Collaborate with CRA Researchers

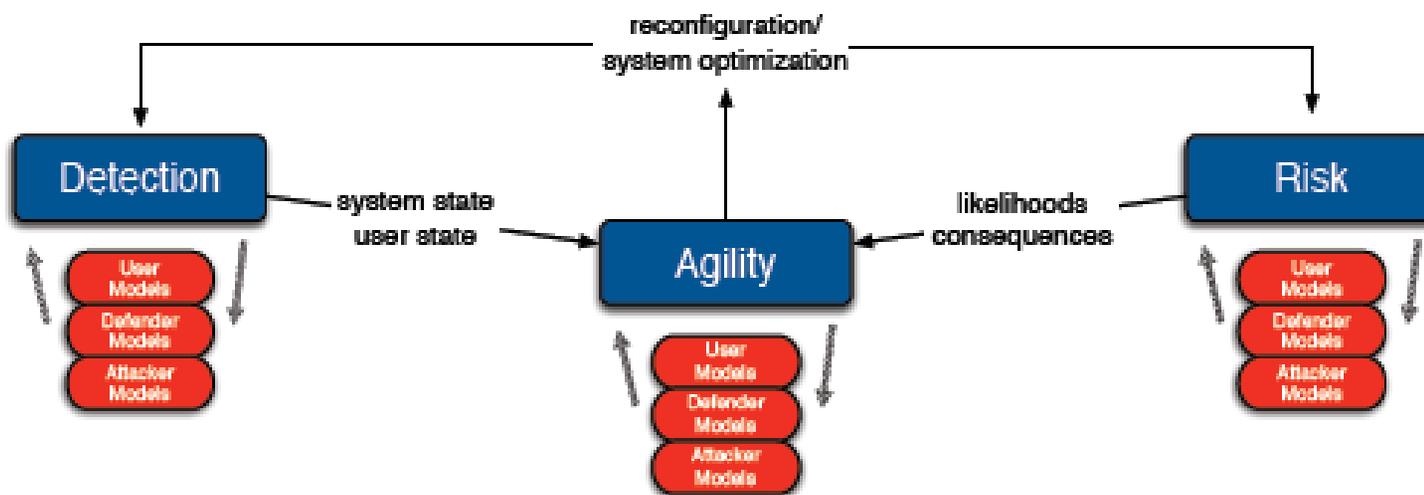


AR&EP Roles



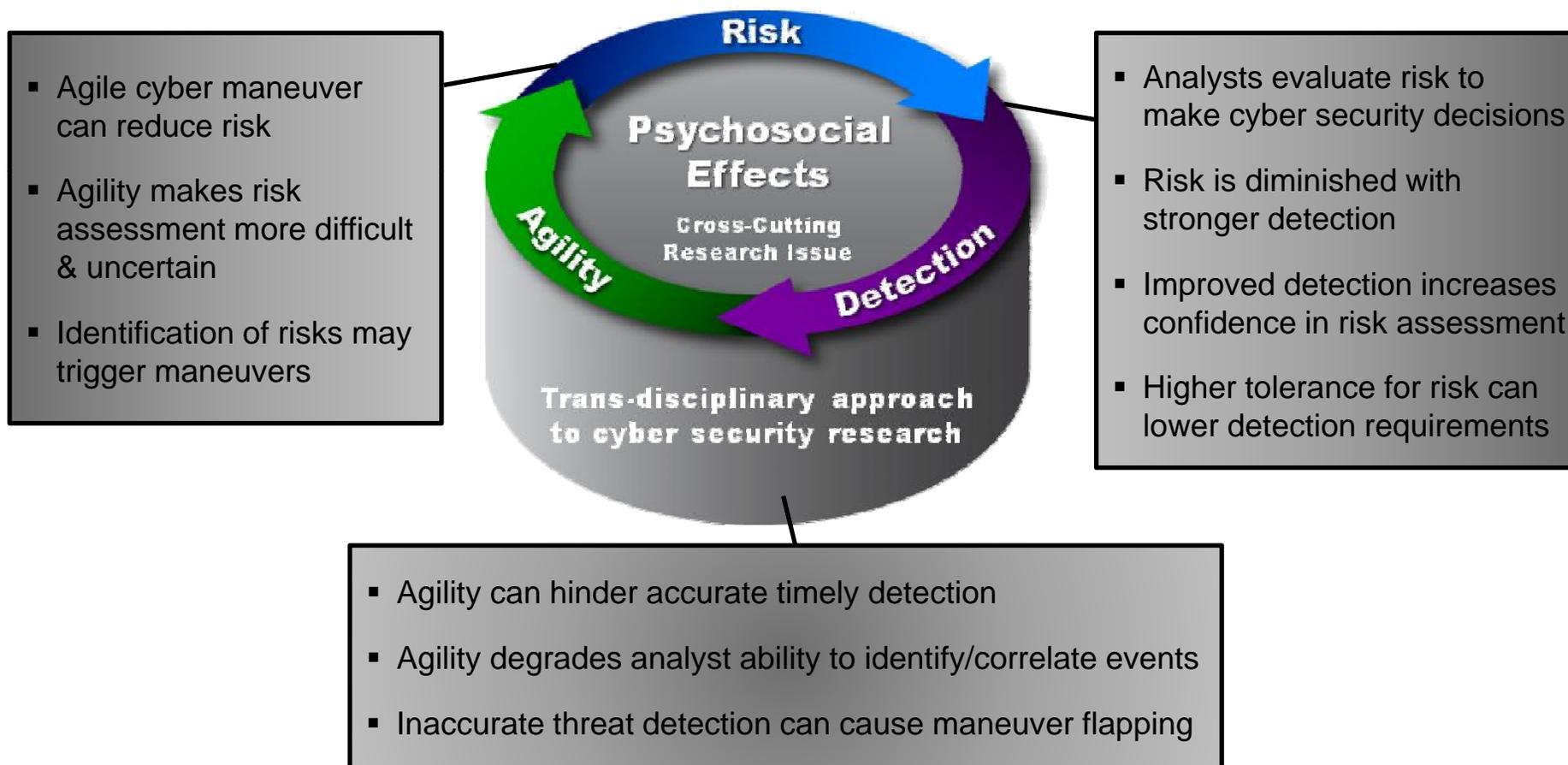
- 1) Evolve basic research (6.1) results to experimental validation
 - Understand the theories/models being developed
 - Return results to ARL/CERDEC
 - Cyber CRA Members, as classification permits
- 2) Perform applied research (6.2)
 - Develop innovative experimental designs
 - Represent complexity & dynamics of Army's cyber domain
 - Improve accuracy, realism, impact, relevance of experimental processes
- 3) Join Cyber CRA
 - Participate as a Consortium Member and perform basic research
 - Actively collaborate; technical publications
 - Maintain effective feedback loop

- Goal: develop a *rigorous science of cyber-security* that will
 - (a) detect the risks and attacks present in an environment
 - (b) understand/predict users, defenders, and attacker action
 - (c) alter the environment to securely achieve maximal mission success rates at the lowest resource cost.



- Outcome: dictate and control the evolution of cyber-missions and adversarial actions

- Risk, Detection, & Agility are intricately linked & co-evolving
- Psychosocial Effects are key to understanding decision making of the user, defender, adversary as they relate to Risk, Detection, & Agility





Cyber Operation Model



Develop formal structures for reasoning about cyber-maneuvers and security goals and strategies. Representations must be decomposable in ways that make analysis tractable.

Operation model development:

- Model the selection of a cyber-maneuver within an operation as a discrete decision problem
- Set of security requirements, security outcomes, risks, costs, and payouts
- Identify model elements that introduce fundamental hardness to decision making in this environment

Reason about strategies that achieve goals while maintaining the security requirements of the mission.



U.S. ARMY
RDECOM[®]
TECHNOLOGY DRIVEN. WARFIGHTER FOCUSED.

ARL



TECHNOLOGY DRIVEN. WARFIGHTER FOCUSED.