Cyber Defense Research Center

Overview

O. Sami Saydjari

June 2000

Challenging Questions

Commander’s Attack Triage Questions

- Am I under attack ?
- What is the nature of the attack ?
  - Class, Mechanism, From where ?
- What is mission impact ?
  - Urgency, Damage assessment & control, Initial response
- When did attack start ?
  - Follow-on damage assessment, What have I done wrong ?
- Who is attacking
  - What are they trying to do, What is their next step ?
- What can I do about it ?
  - Course of action analysis, Collateral damage risk, Reversibility of action
- Long term solution

Currently, we are ***Blind*** and ***Powerless*** at all echelons

CyberDefense Need

United States is blind and powerless against sophisticated attack

Four Basic Needs

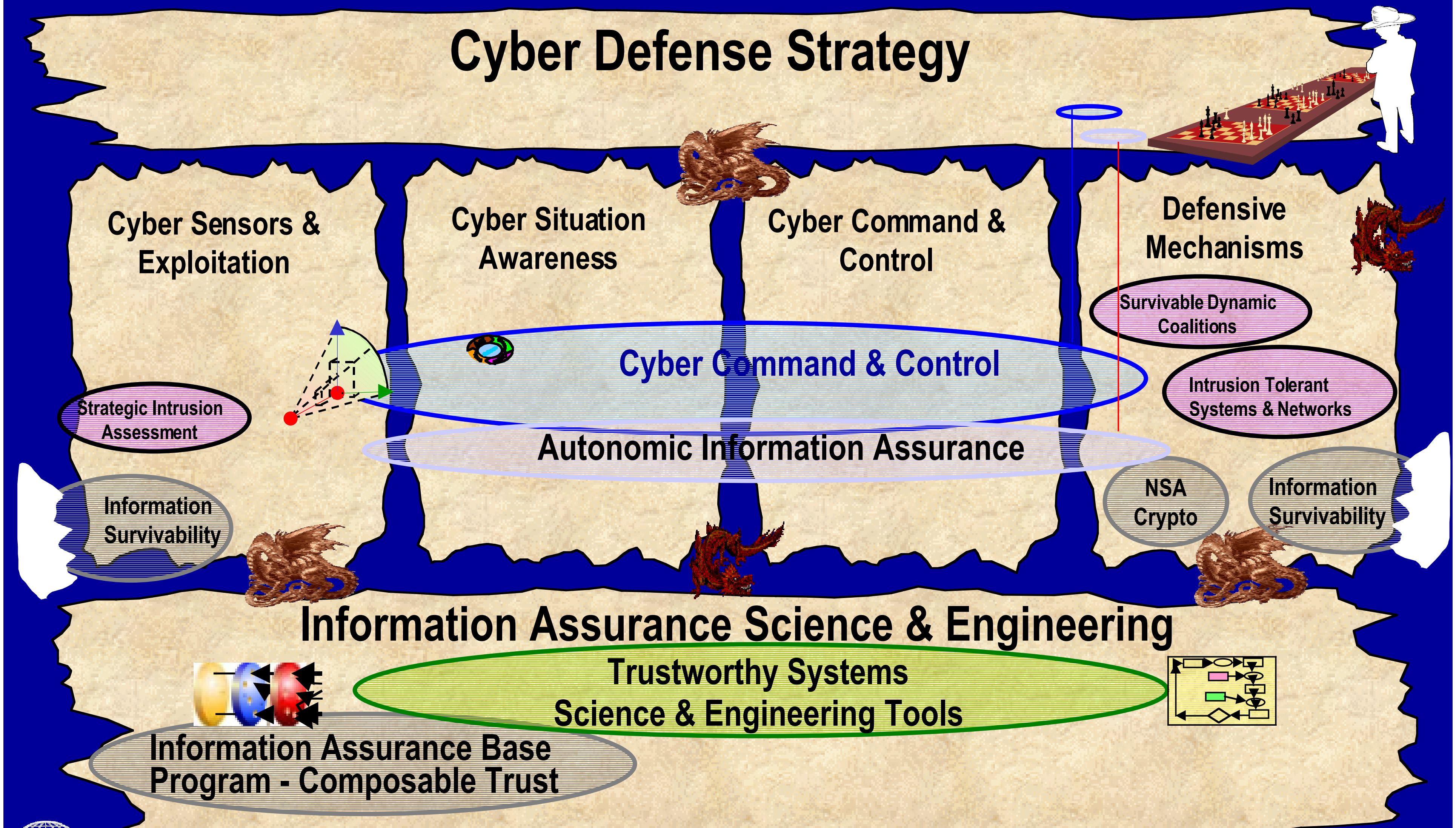
1. **See** – Situation Understanding

2. **Act** – Command and Control

3. **Build** –Tools

4. **Share** – Policy

Strategic Cyber Defense - A Map History



Cyber Defense Strategy

Cyber Sensors & Exploitation

Cyber Situation Awareness

Cyber Command & Control

Defensive Mechanisms

Survivable Dynamic Coalitions

Intrusion Tolerant Systems & Networks

Strategic Intrusion Assessment

Cyber Command & Control

Autonomic Information Assurance

Information Survivability

NSA Crypto

Information Survivability

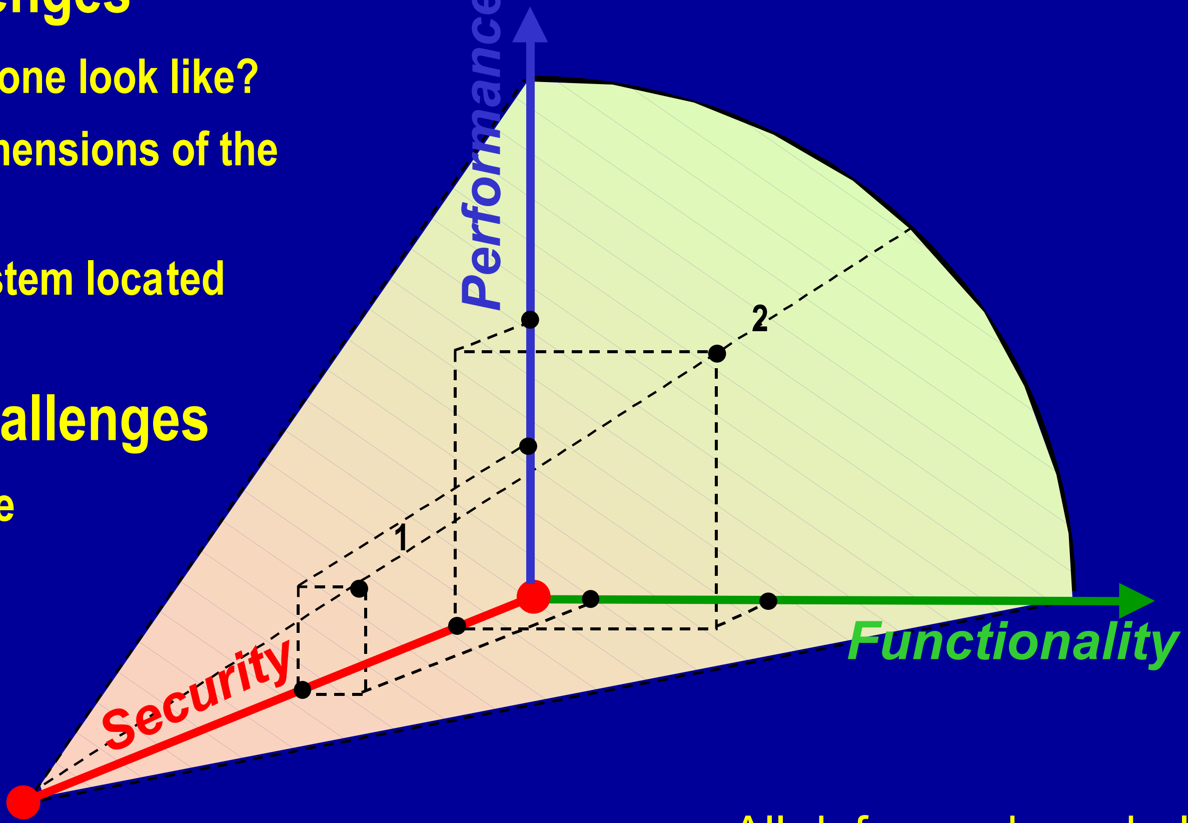
Information Assurance Science & Engineering

Trustworthy Systems Science & Engineering Tools

Information Assurance Base Program - Composable Trust

The Challenge: How to Maneuver in Cyberspace

- **Systems Challenges**
  - What does the cone look like?
  - What are the dimensions of the tradeoff space?
  - Where is the system located on the cone?
- **Technology Challenges**
  - Dynamic, flexible mechanisms
  - Rapid & random reconfigurability

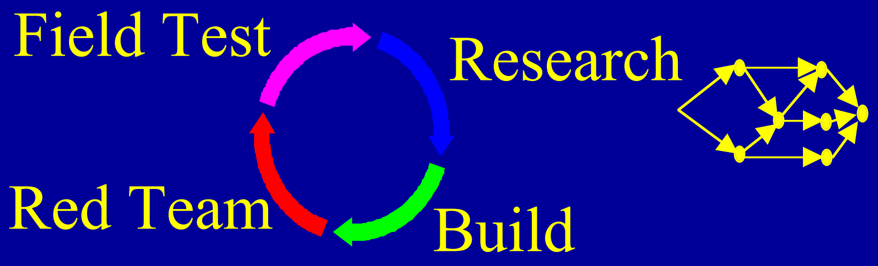


Confidentiality, Integrity, Availability

- All defenses have holes.
- All software has bugs.
- Static systems risk being sitting ducks.

CyberDefense Research Center Need

- **Multidisciplinary approach needed --> new discipline**
  - emphasis on experimental methods on real-world problems
  - deeply inter-related research orchestration easier in one place



Field Test

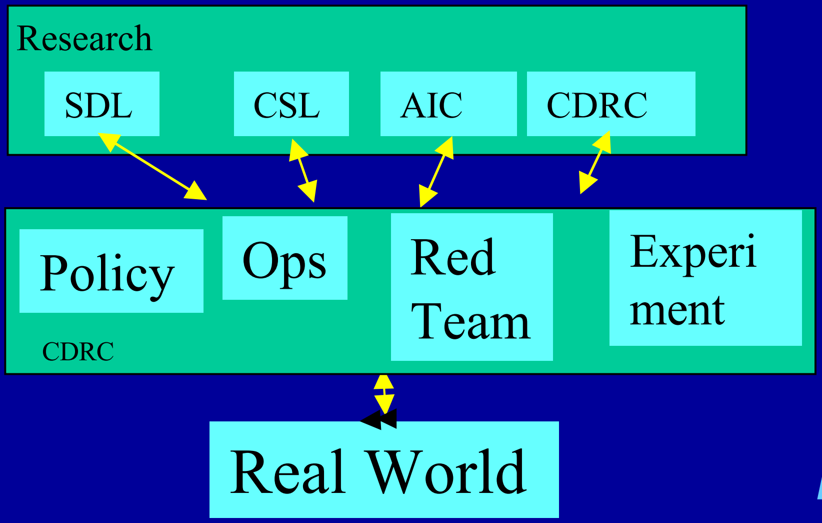
Research

Red Team

Build

CDRC as Technology Bridge

- Create system test environment with driving apps
  - technology folk will WANT to integrate in to use environment
  - operational folks will want to offer driving data-sets for insight into emerging technology
- Once tested in CDRC lab– do *field experiments*



Research

Transition

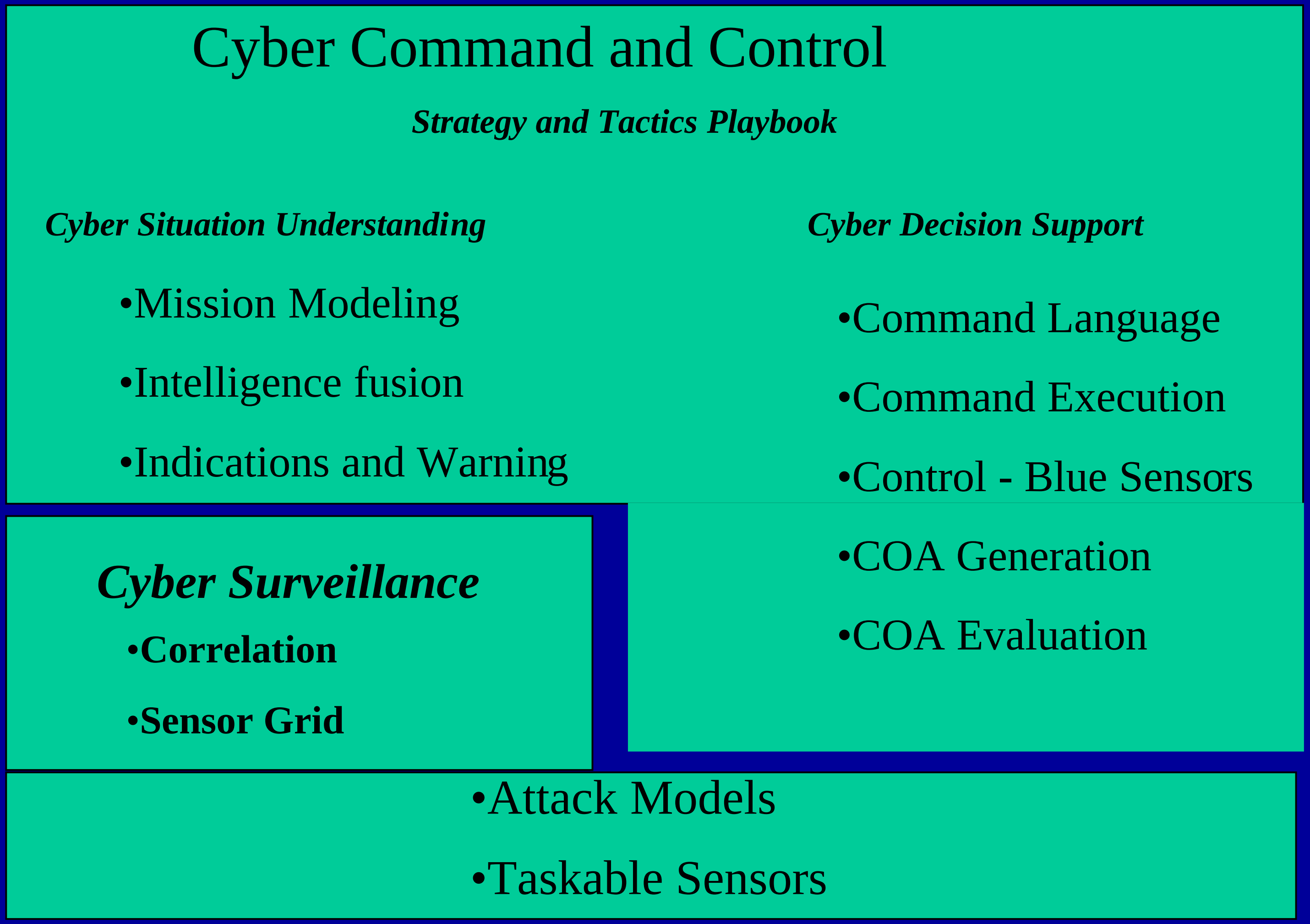
Deploy & Create Value

Approach: See

Now: Detect Local Known *Exploits* → Future: Detect Distributed Novel *Attacks*

- **See –[SIA, CC2] = Cyber Situation Understanding Subsystem**
  - build on Emerald (bottom up) and recent e-bayes extension +
  - (top-down) command and control & fusion expertise in AIC... to create

Some Operational BIG Issues



Cyber Command and Control

Strategy and Tactics Playbook

Cyber Situation Understanding

- Mission Modeling
- Intelligence fusion
- Indications and Warning

Cyber Decision Support

- Command Language
- Command Execution
- Control - Blue Sensors
- COA Generation
- COA Evaluation

Cyber Surveillance

- **Correlation**
- **Sensor Grid**

- Attack Models
- Taskable Sensors

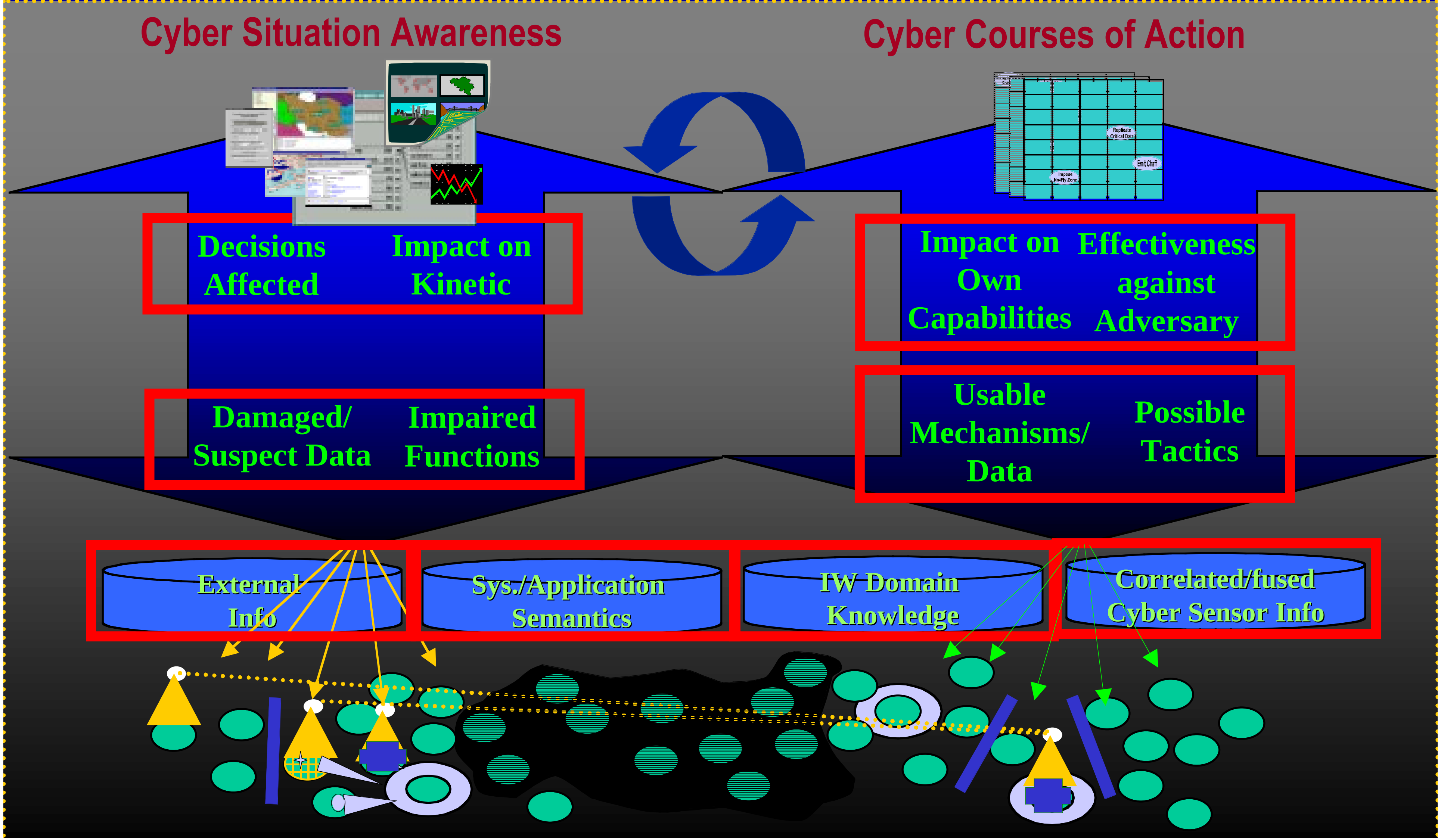
Objectives ->Strategy -> Decisions -> Understanding -> Surveillance

Approach: Act

Now: Manual Mechanism Reconfig → Future: Auto System Orchestrated Response

- **Act – [CC2, AIA] = Cyber Decision Support Subsystem**
  - address operator frustrations in orchestration– simple tools in near-term
  - work control theory for analogies, principles, tools to apply to the problem
  - Sponsor war-gaming sessions to work tactics and strategy
  - Apply AIC decision tools from traditional C2 to Cyber arena --> RUBY
  - Cyberwar Playbook and Synthetic Cyberwargaming Environment

Cyber Command & Control (CC2)



Cyber Situation Awareness

Cyber Courses of Action

Decisions Affected

Impact on Kinetic

Damaged/ Suspect Data

Impaired Functions

Impact on Own Capabilities

Effectiveness against Adversary

Usable Mechanisms/ Data

Possible Tactics

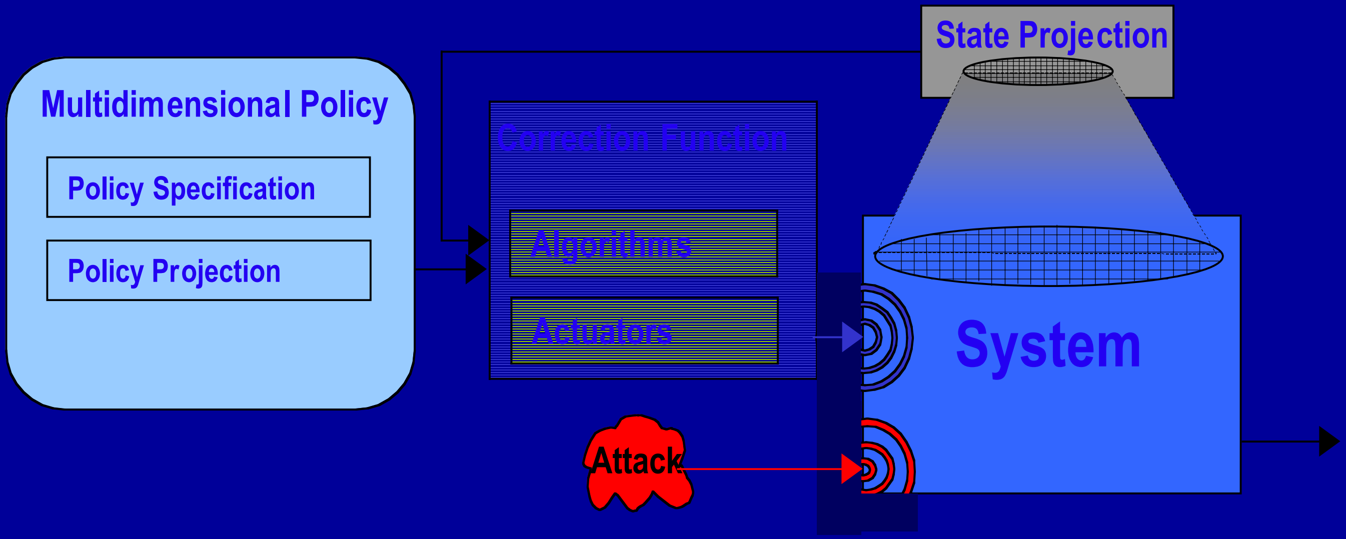
External Info

Sys./Application Semantics

IW Domain Knowledge

Correlated/fused Cyber Sensor Info

Autonomic Information Assurance Approach - Technologies



- Control systems for directing adaptive defense
- Modeling is imperative
- Correction Function
- Multidimensional Policy
- State Estimation

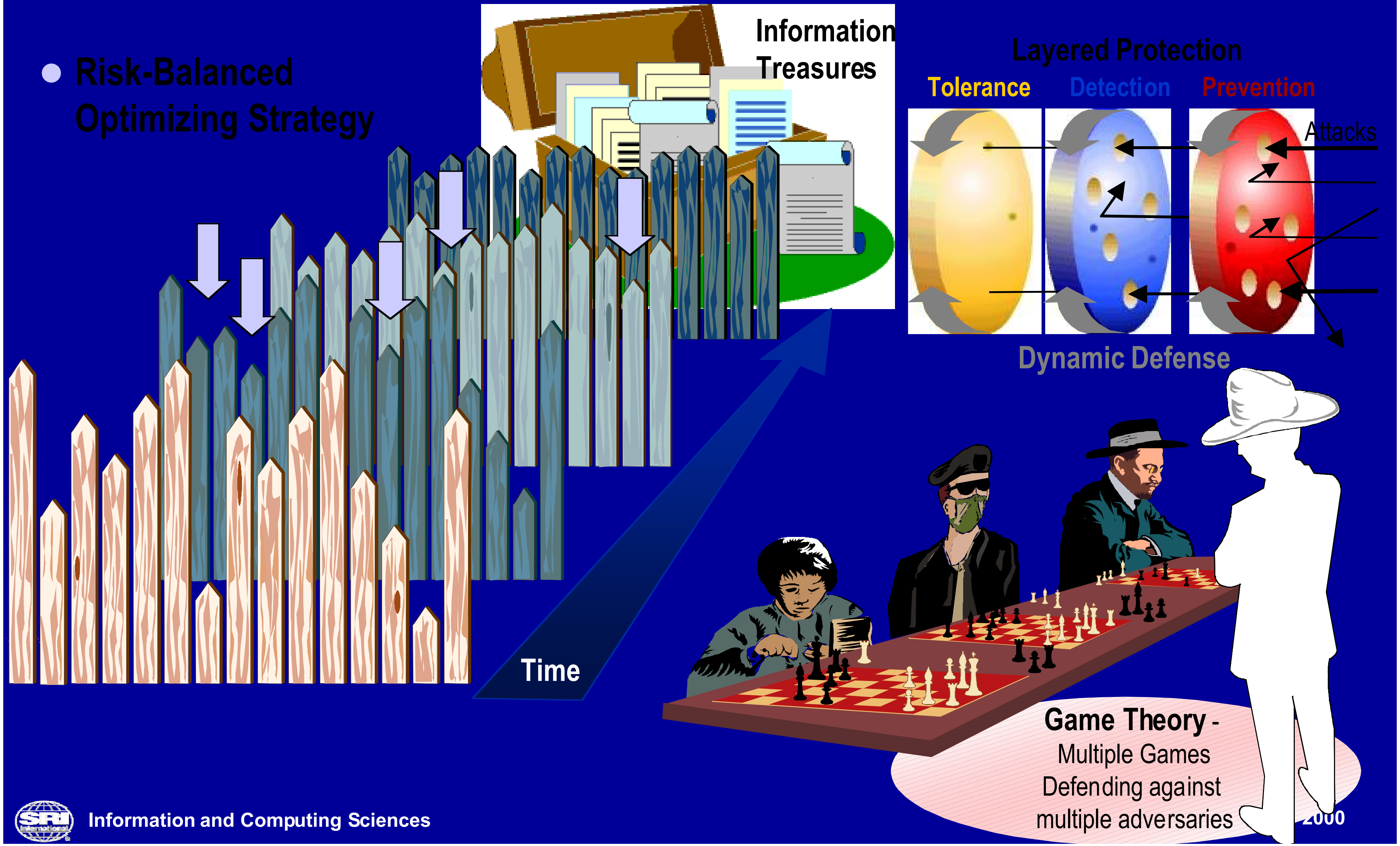
Approach: Build

Now: Black Art Design By Exhaustion → Future: Engineered Assurance Properties

- **Build – [IASET] = Security Engineer's CAD system**
  - Analysis Thrust – Create World's Best Red Team
    - **Apply red-teams against research systems - Research IV&V**
    - **View red-teams as clients - effectiveness by creating tools/knowledge**
    - **Set up experiments to discover effective defense strategies**
  - Design Thrust – Create a Security Codesign Workbench
    - **Capitalize on existing SDL in-house expertise**
    - **create vulnerability + countermeasure effectiveness models**
    - **work on design methodology & begin populating method with tools**

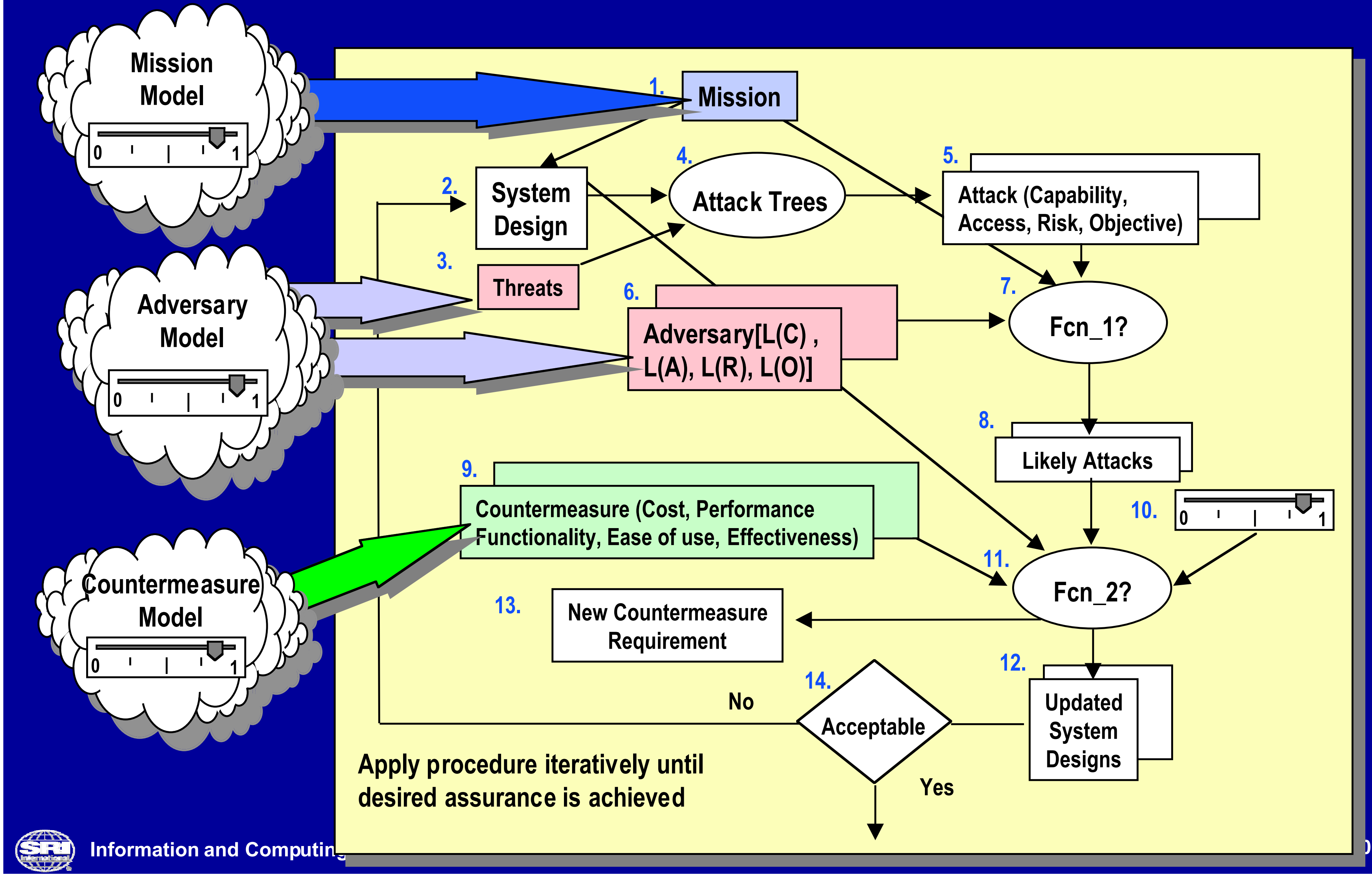
Information Assurance Approach

- Risk-Balanced Optimizing Strategy



Game Theory - Multiple Games Defending against multiple adversaries

System Level Assurance Methodology



Mission Model

Adversary Model

Countermeasure Model

1. Mission

2. System Design

3. Threats

4. Attack Trees

5. Attack (Capability, Access, Risk, Objective)

6. Adversary[L(C) , L(A), L(R), L(O)]

7. Fcn_1?

8. Likely Attacks

9. Countermeasure (Cost, Performance Functionality, Ease of use, Effectiveness)

10.

11. Fcn_2?

12. Updated System Designs

13. New Countermeasure Requirement

14. Acceptable

No

Yes

Apply procedure iteratively until desired assurance is achieved

Contrast of **breadth** versus depth of defense.

- Red Team 9901

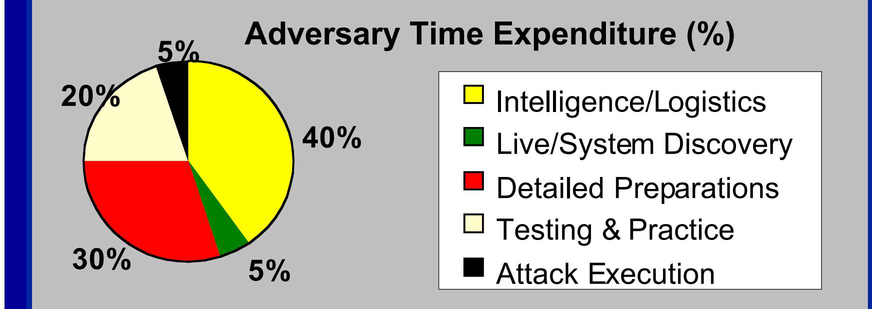
Depth: Multiple mechanisms against an attack class
Breadth: Multiple mechanisms across attack classes

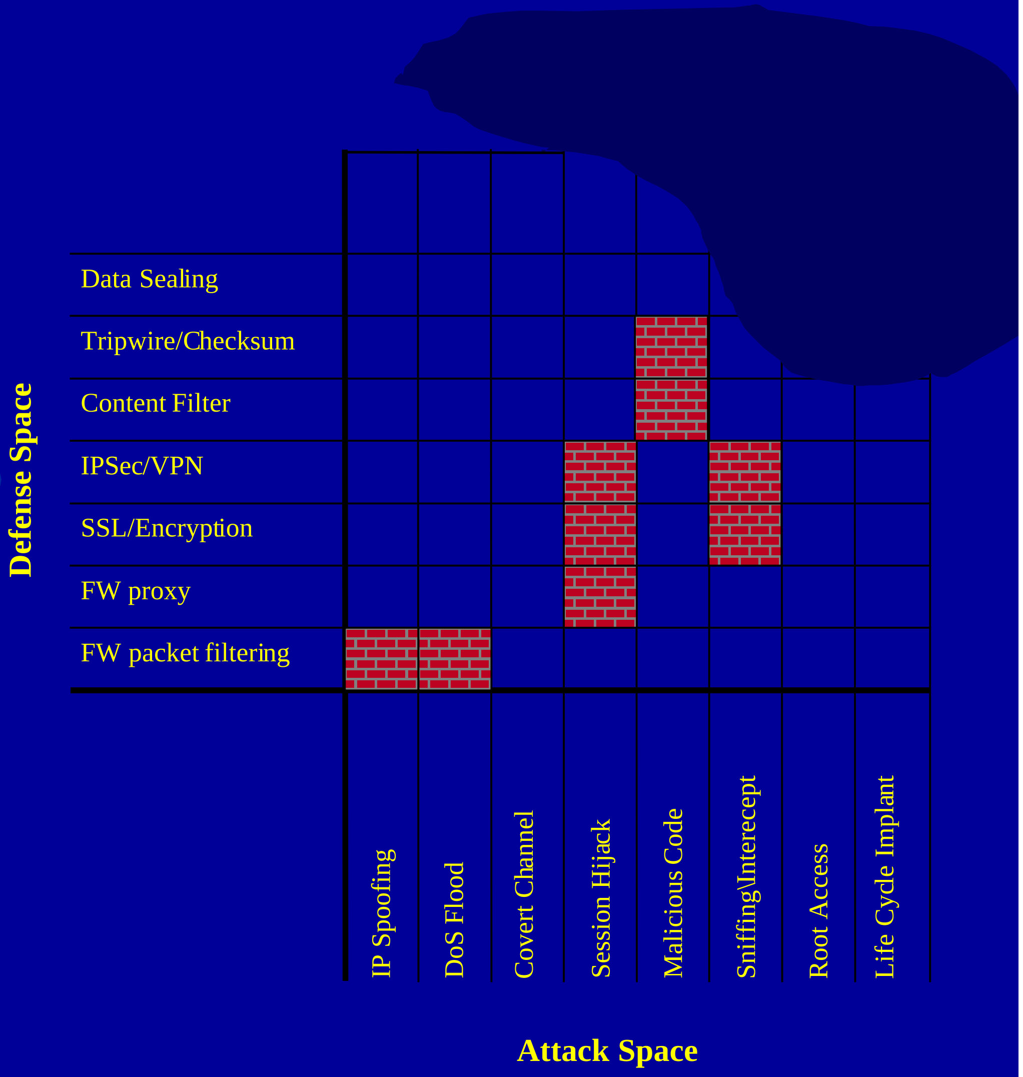
Hypothesis: Adding layers has at least a cumulative impact on adversary work factor

Compare attacker work factors as more defense/prevent layers are added in a client-server database architecture

- **Depth without breadth is useless**
- Individual layers may address specific attacks
- Layers can move attack points to manageable places
- Dependencies of layers must be enforced

- Red Team 9903





	IP Spoofing	DoS Flood	Covert Channel	Session Hijack	Malicious Code	Sniffing\Intercept	Root Access	Life Cycle Implant
Data Sealing								
Tripwire/Checksum					▨			
Content Filter					▨			
IPSec/VPN				▨		▨		
SSL/Encryption				▨		▨		
FW proxy				▨				
FW packet filtering	▨	▨						

Approach : Share

Now: Isolated all-or-none Sharing → Future: Selected Controlled Collaboration

- **Share – [DC, ITS, FTN] = Private Cyberspaces**
  - re-think policy in much broader context of a control problem
  - work policy specification requirements specification language problem
  - create, instrument, and mediate private cyberspaces
  - Create Unified Policy Trade-off Framework

BACKUP

For Video Copies...
Ghamilton@snap.org