The Decision Professionals Network

SDP

DAS Decision Analysis Society

Rethinking Decision Analysis

Greg Parnell

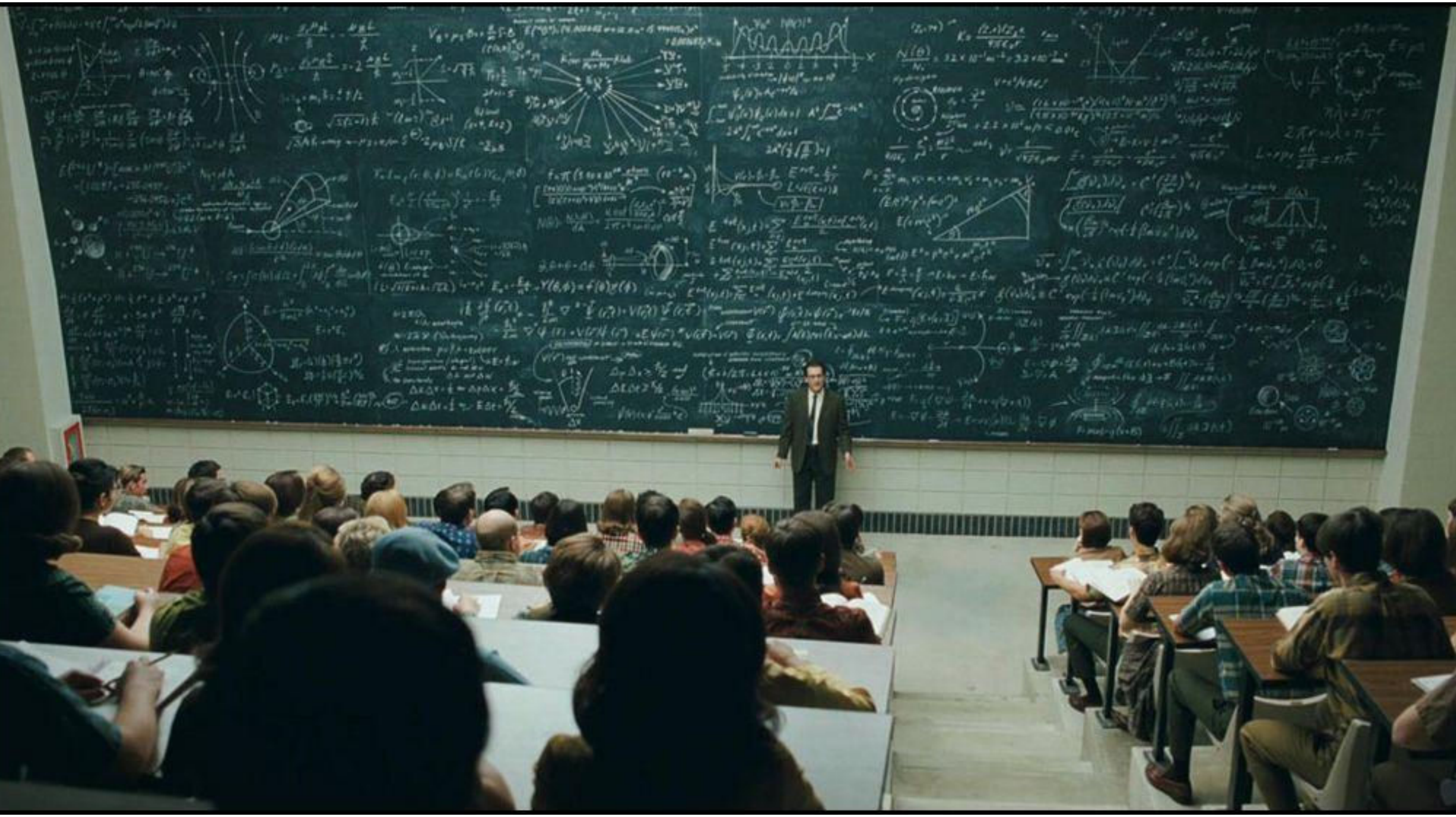
SMDM Society for Medical Decision Making

MORS MILITARY OPERATIONS RESEARCH SOCIETY

INCOSE INTERNATIONAL COUNCIL ON SYSTEMS ENGINEERING

Lean Systems Society

This presentation will be easy to follow.



Decision Analysis Handbook

Wiley & Sons OR/MS Handbook Series

Submit to the publisher 1 Aug 12

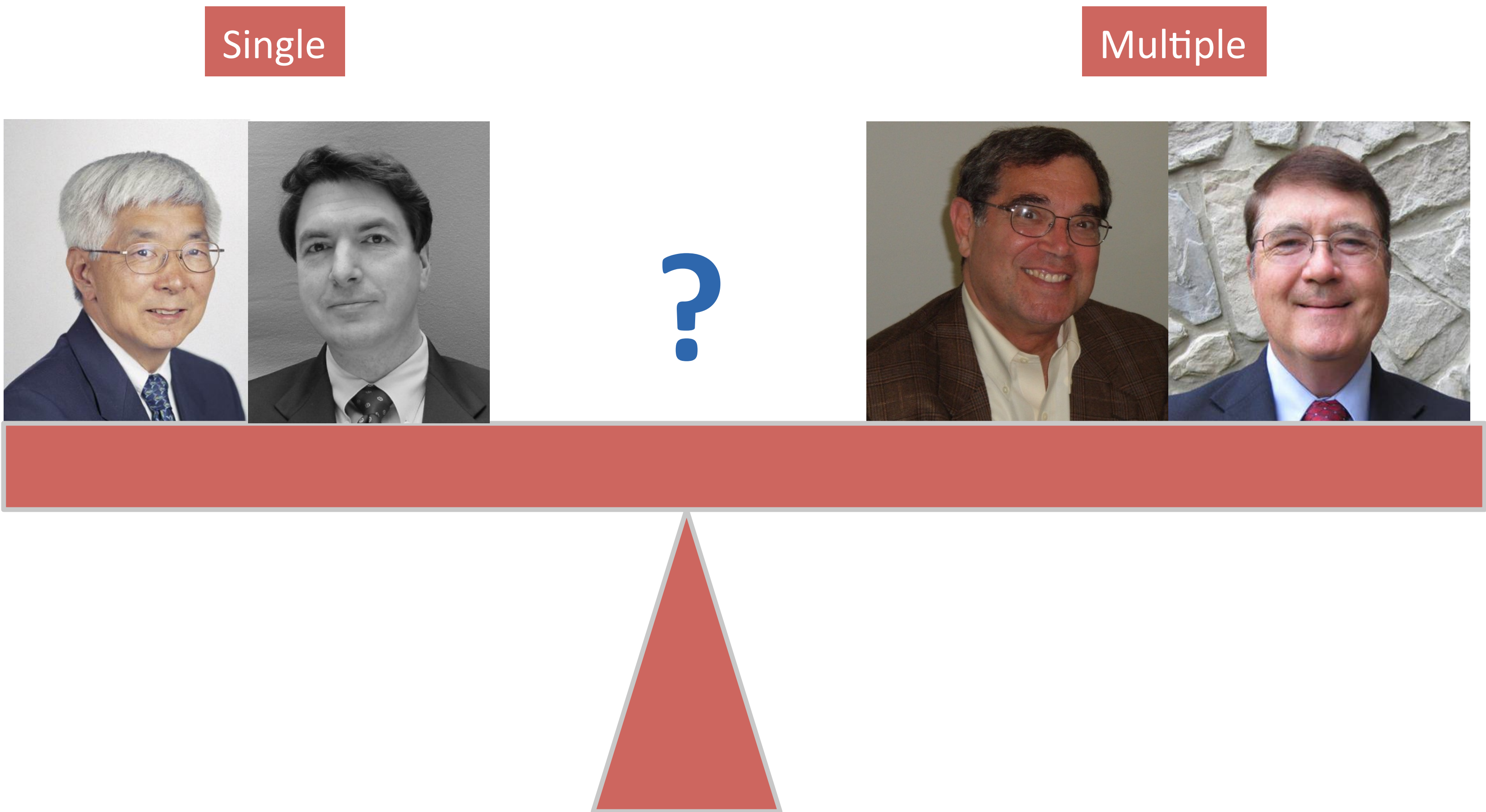
- SDG Partner and Fellow
- Over 35 years of DA experience
- Private and public
- Professional courses

- Founder, past President of IDI
- Over 35 years of DA experience
- Public (military, intel, etc) and private
- Professional courses

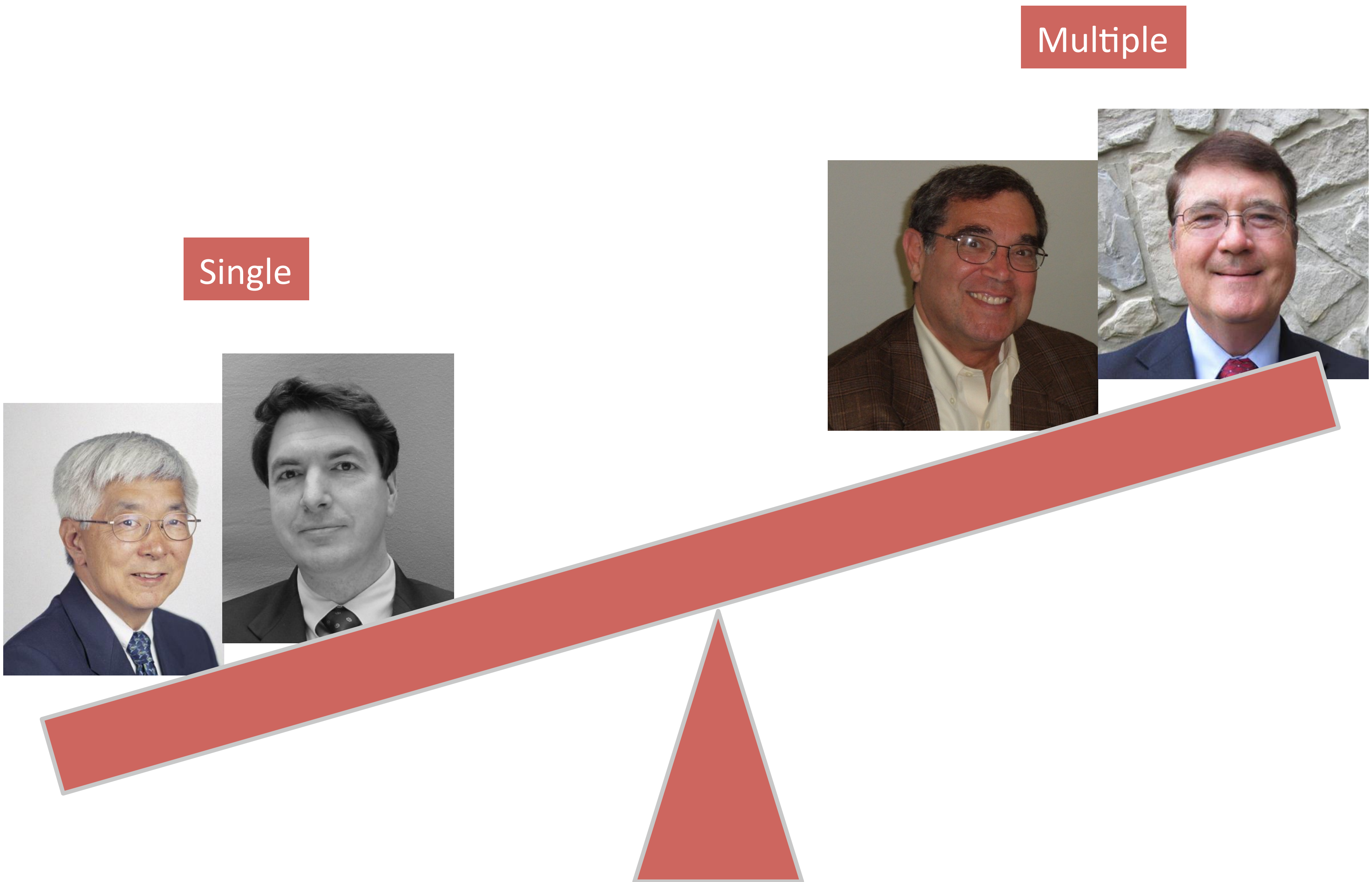
- BMS
- Internal and external (Decision Strategies)
- DA experience in pharmaceuticals, oil and gas and electric utilities

- Professor, West Point
- Internal analysis leader and consultant at IDI
- Over 35 years of DA experience
- Public (military, intel, homeland security, etc.)
- Professional courses

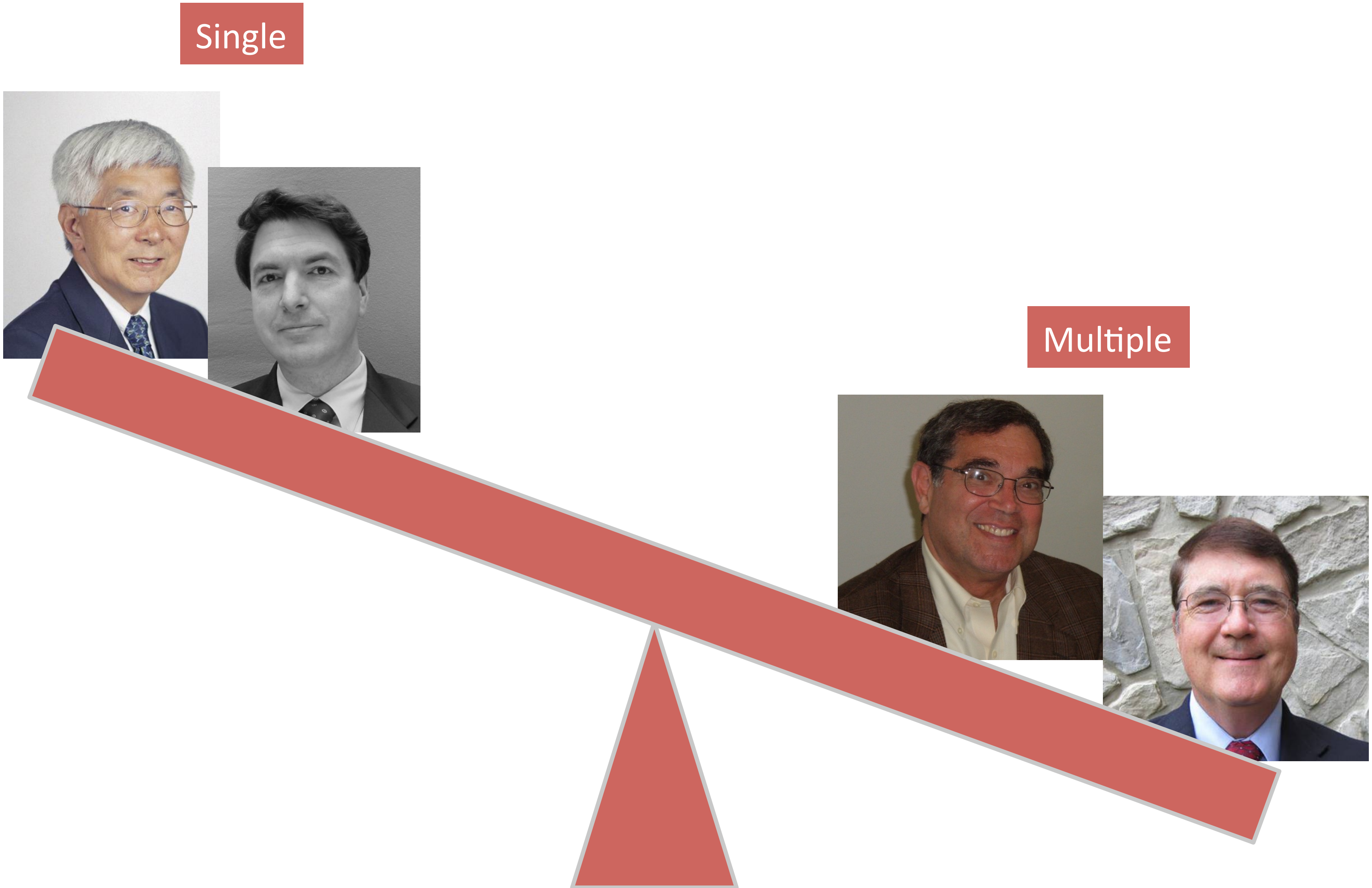
How to balance single and multiple objective decision analysis?



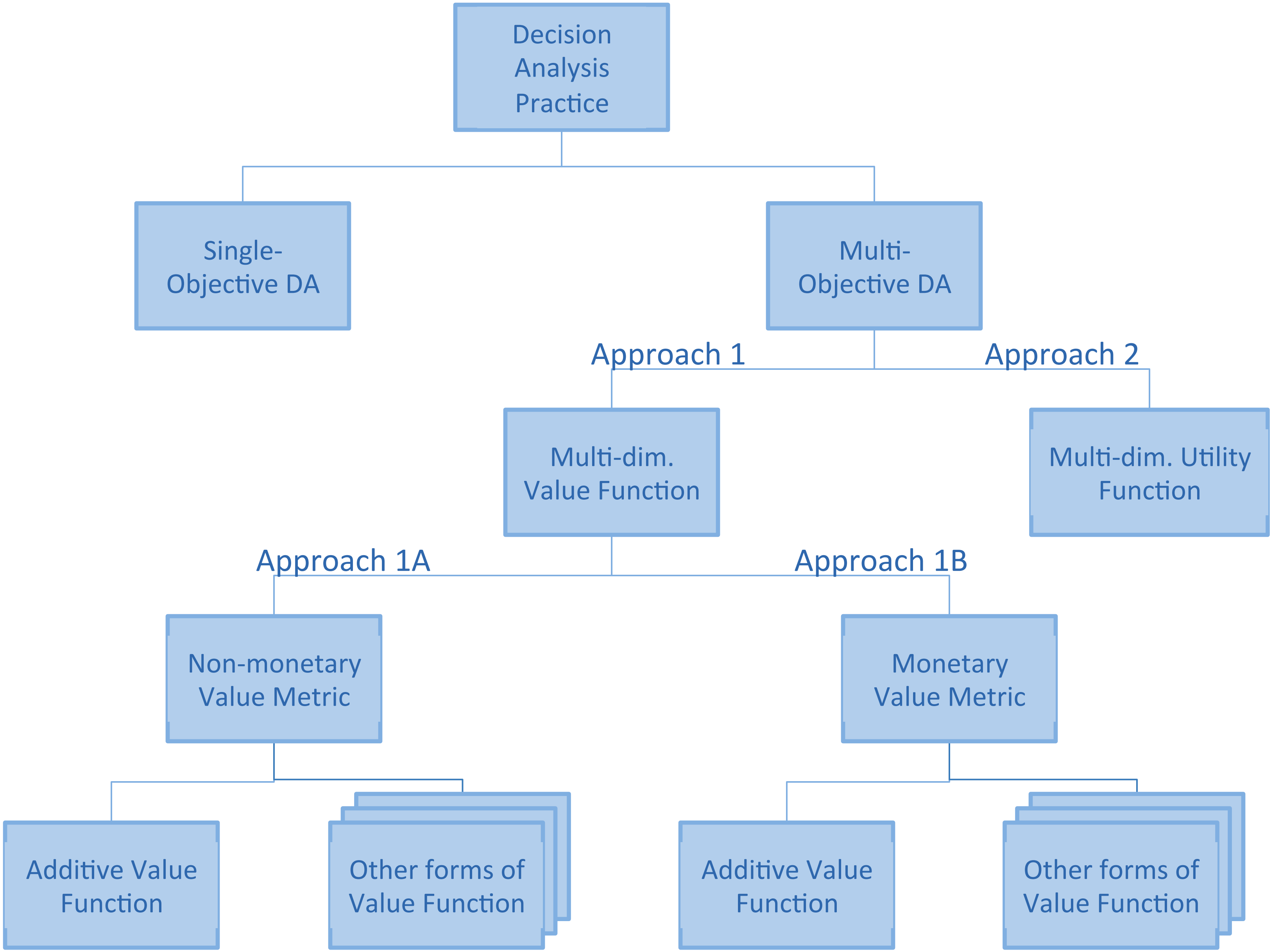
Chronological

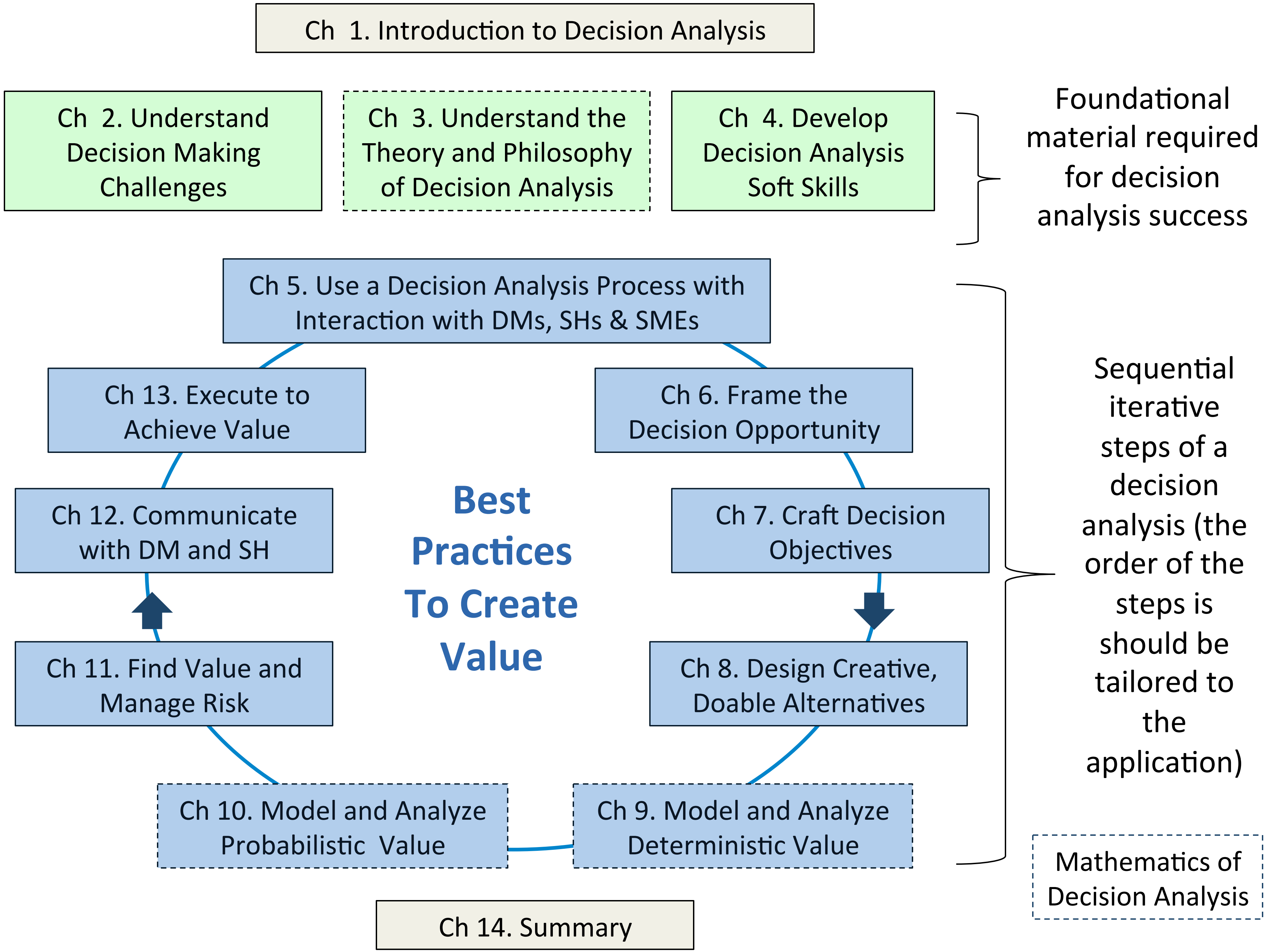


General and special case.



Tani’s Taxonomy of Decision Analysis Practice




Ch 1. Introduction to Decision Analysis
Ch 2. Understand Decision Making Challenges
Ch 3. Understand the Theory and Philosophy of Decision Analysis
Ch 4. Develop Decision Analysis Soft Skills
Foundational material required for decision analysis success
Ch 5. Use a Decision Analysis Process with Interaction with DMs, SHs & SMEs
Ch 6. Frame the Decision Opportunity
Ch 7. Craft Decision Objectives
Ch 8. Design Creative, Doable Alternatives
Ch 9. Model and Analyze Deterministic Value
Ch 10. Model and Analyze Probabilistic Value
Ch 11. Find Value and Manage Risk
Ch 12. Communicate with DM and SH
Ch 13. Execute to Achieve Value
Best Practices To Create Value
Sequential iterative steps of a decision analysis (the order of the steps is should be tailored to the application)
Mathematics of Decision Analysis
Ch 14. Summary

Soft Skills of Decision Analysis

- **Leading** teams including developing analysis plans, scheduling activities, and managing the completion of tasks
- **Researching** the problem domain, modeling approaches, and data sources.
- **Interviewing** individuals (DMs, SHs and SMEs) to frame the decision problem and obtain modeling information.
  - Interact with senior leaders and SMEs
  - Elicit knowledge (preferences [value, time, and risk], probabilities, alternative)
- **Facilitating** groups of SMEs and SHs
  - Frame decision opportunity (initial and updated)
  - Elicit knowledge (preferences [value, time, and risk], probabilities, alternative)
  - Use individual and group creativity techniques (values, sources of risk, strategy design, strategy improvement)
- **Communicating** with to DMs, SHs, and SMEs
  - Communicate the story, analytic results, and the key insights in ways that are understandable to the audience.

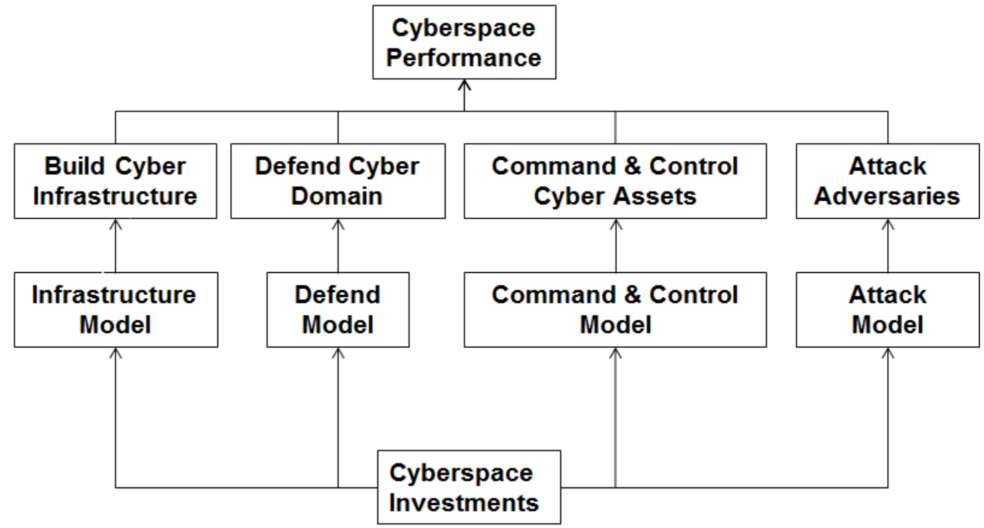
AFSPC Cyberspace Value Model

Mike Tedeschi, USNORTHCOM/J8
Steve Wichmann, AFSPC/A9FP
Reb Butler, AFSPC/A8XP
Dr. Lee Lehmkuhl, MITRE
Donald Aiken, SCITOR
John Wright, USNORTHCOM/J8
Joel Swisher, A3I
Dr. Greg Parnell, USAFA/DFM
Dr. Jim Lowe, USAFA/DFM
Maj David Merritt, USAFA/DFM

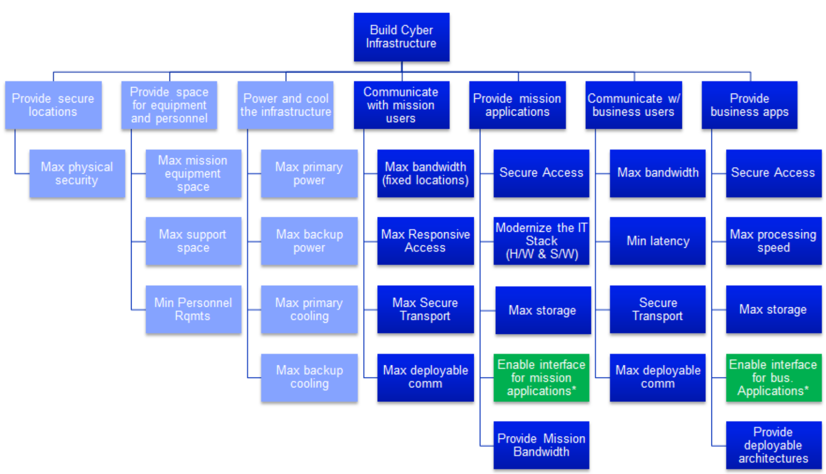
Bottom Line Up Front

- Cyberspace operations are a primary mission of the U.S. Armed Forces
- Air Space Command performs investment planning for Air Force space and cyberspace missions
- We developed and implemented an improved cyberspace model to support AFSPC investment planning for $3.5B portfolio

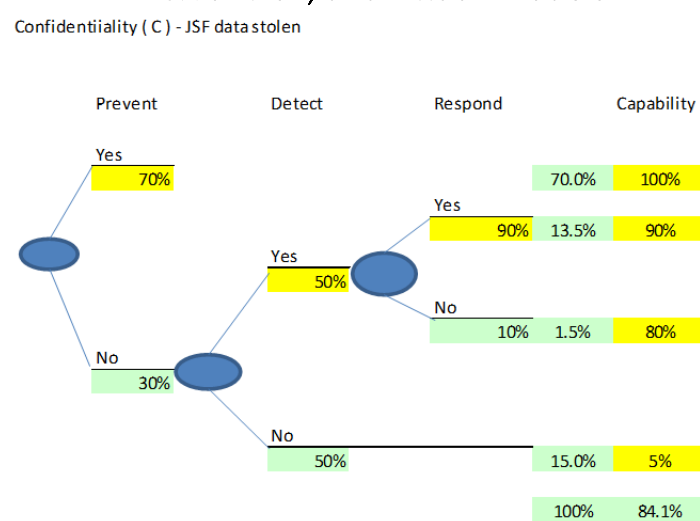
Cyberspace Value Model Concept



Use Multiple Objective Decision Analysis (MODA) for Infrastructure Model



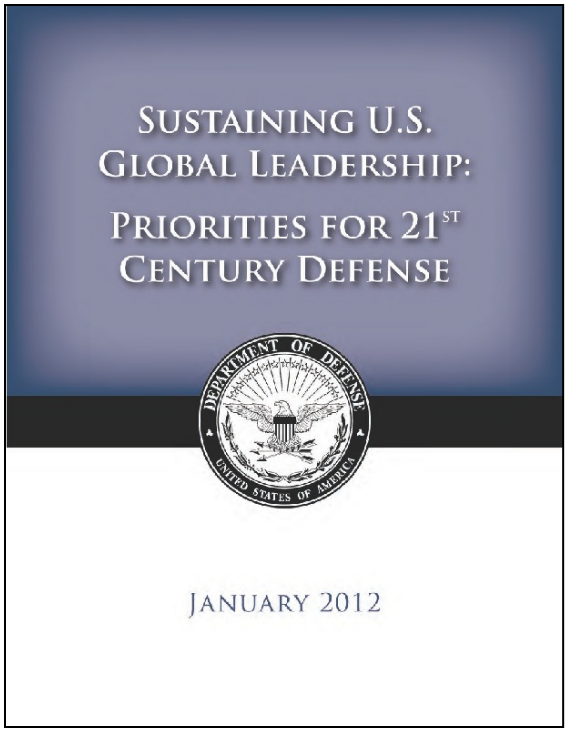
Use Probabilistic Analysis for Defend, Command &Control , and Attack Models



Overview

- Cyberspace mission
- Air Force Space Command Investment Planning Process (IPP)
- Cyberspace Value Model
  - Analytical challenges
  - Decision hierarchy
  - Cyberspace model concept
  - Cyberspace models
- Integration into Air Force Space Command IPP

A Primary Mission of the U.S. Armed Forces



Operate Effectively in Cyberspace and Space

"Modern armed forces cannot conduct high-tempo effective operations without reliable information and communications networks and assured access to cyberspace and space. Today space systems and their supporting infrastructure face a range of threats that may degrade, disrupt, or destroy assets. *Accordingly, DoD will continue to work with domestic and international allies and partners and invest in advanced capabilities to defend its networks, operational capability, and resiliency in cyberspace and space*."

Page 5

Investment Planning Process (IPP)

Air Force Space Command force structure based on rigorous enterprise-wide assessment

- Considers threats and perils of a future operating environment
- Considers reasonable fiscal projections capability shortfalls, and system solutions that maximize warfighting effects
- Considers major shifts in capability strategies

INPUT

National, DoD & Joint Imperatives

AF Strategic & Guidance Plan

CC Strategic Plan

Capability Area Analysis - Define and Prioritize Capabilities	Capability Needs Analysis - Determine Shortfalls	Capability Solutions Analysis - Develop Concepts	Integrated Investment Analysis - Produce Roadmaps
Integrated and Prioritized Capability List Capability Measures	Prioritized Shortfalls and Gaps Supports IPL, CRRA, S&T and developmental planning	Catalog of all potential solutions to satisfy capabilities ID'd in CAA	Final Details for optimal capability delivery given fiscal constraints

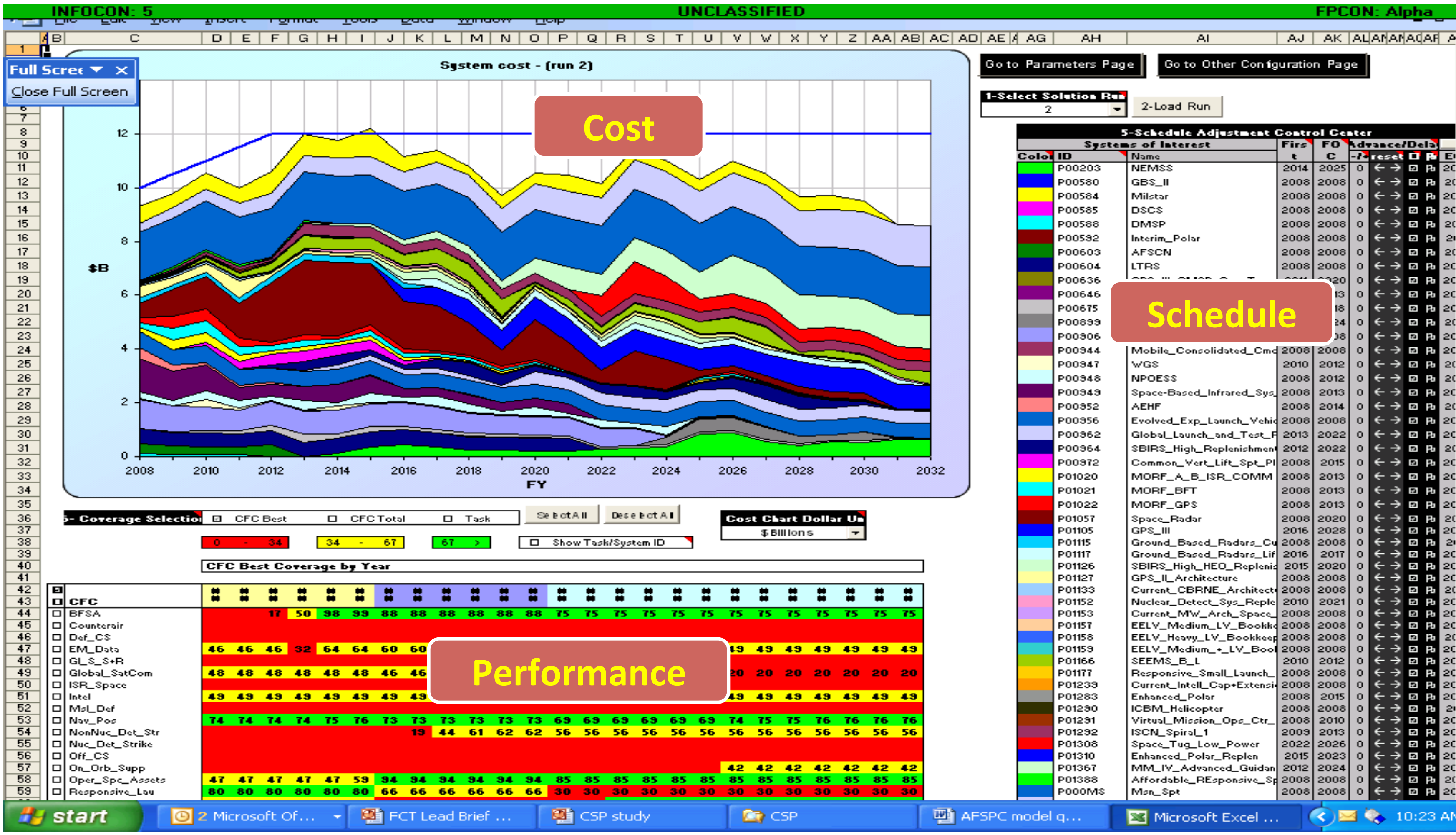
PROCESS OUTPUTS

Core Function Master Plans

Air Force Space Command Strategic Plan

IPP uses decision analysis and optimization to analyze performance, cost, and schedule trade offs

Notional data that shows a force mix under a fixed budget.



Space and Cyberspace have very different analytical challenges

Factor	Space	Cyberspace
Threat	Environmental Potential ASAT systems	Continuous Growing
Threat resources	Peer nation state	Nation state, Group (e.g., Terrorist) Individual
Infrastructure	Discrete launch, space segments, ground segments, and communications	Ubiquitous IT hardware, software and communications
Technology change	Many years to design and deploy	Rapid change (Moore's Law)
Technical performance	Established technical measures for each space system	IT measures (e.g., processing speed, storage, bandwidth)
Operational	Known operational measures and common use of space system operational models.	Poorly defined measures. Some model development for attack planning and some system modeling for defensive capability for specific systems.
Operational modeling of Campaign impact	Some progress in campaign models and Space Brawler development.	No known models
Analytical framework to support investment planning	Evolving model of space capabilities and optimization model of space launch capabilities to ensure feasibility.	Initial model of cyberspace capabilities used in last IPP.

Tenets for Cyberspace Investment Planning Analysis

- Infrastructure
  - Ubiquitous IT hardware, software, and communications
  - Complex network designs and interactions
  - Continuous changes make detailed network modeling for long time horizons problematic
  - Unknown future scenarios
- Threat
  - Adaptive threat is continuous and growing
  - May not be able to defeat all attacks
  - Must design for resiliency (graceful degradation)
- Decision cycles
  - Attack and defense – real-time
  - Infrastructure – daily
  - Procurement – yearly
  - Technology – Moore's Law
  - Resource allocation planning – 2 – 20 years

Cyberspace Analytic Framework will need to rely on aggregate modeling of the functions of mission structure and expert judgment of future threats, vulnerabilities and capabilities to support resource allocation decision making.

Subjective Judgments: When possible we will seek absolute judgments. However, we may have to rely on relative judgments for some measures.

Cyberspace Decision Hierarchy

Done Deals
Decisions, policy already made

- Air Force cyberspace mission
- Investments for FY15-34 with focus on FY15-24
- Use AF Ops Strategy (if affordable)
- Use Air Force Space Command IPP process
- Cyberspace needs sound analytic foundation for investment decision making

Our Decision Focus
Strategic decisions to be made

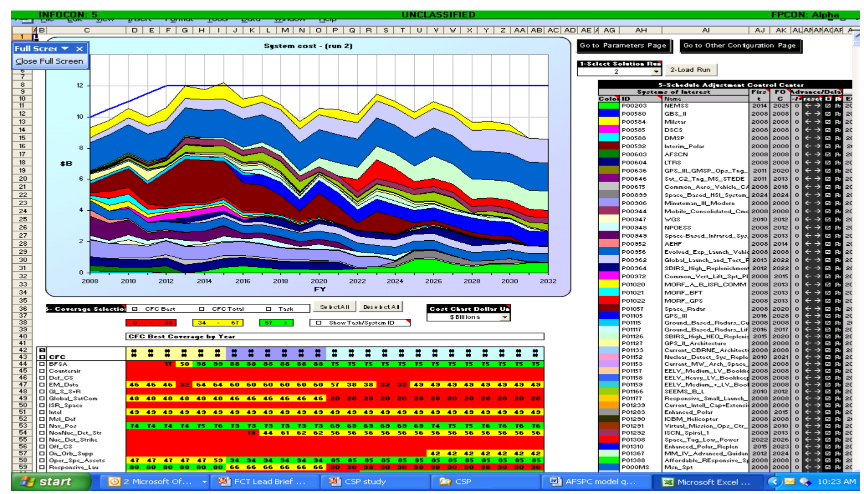
- Consider future cyberspace threats, DOTMLPF opportunities, strategies, architectures, and capabilities
- **Determine the best AF cyberspace investment strategy for varying budget levels**
- Assess the capability and risks at each budget level to inform cyberspace investment decision making

Subsequent Decisions
Tactical or implementation decisions to be made in the future

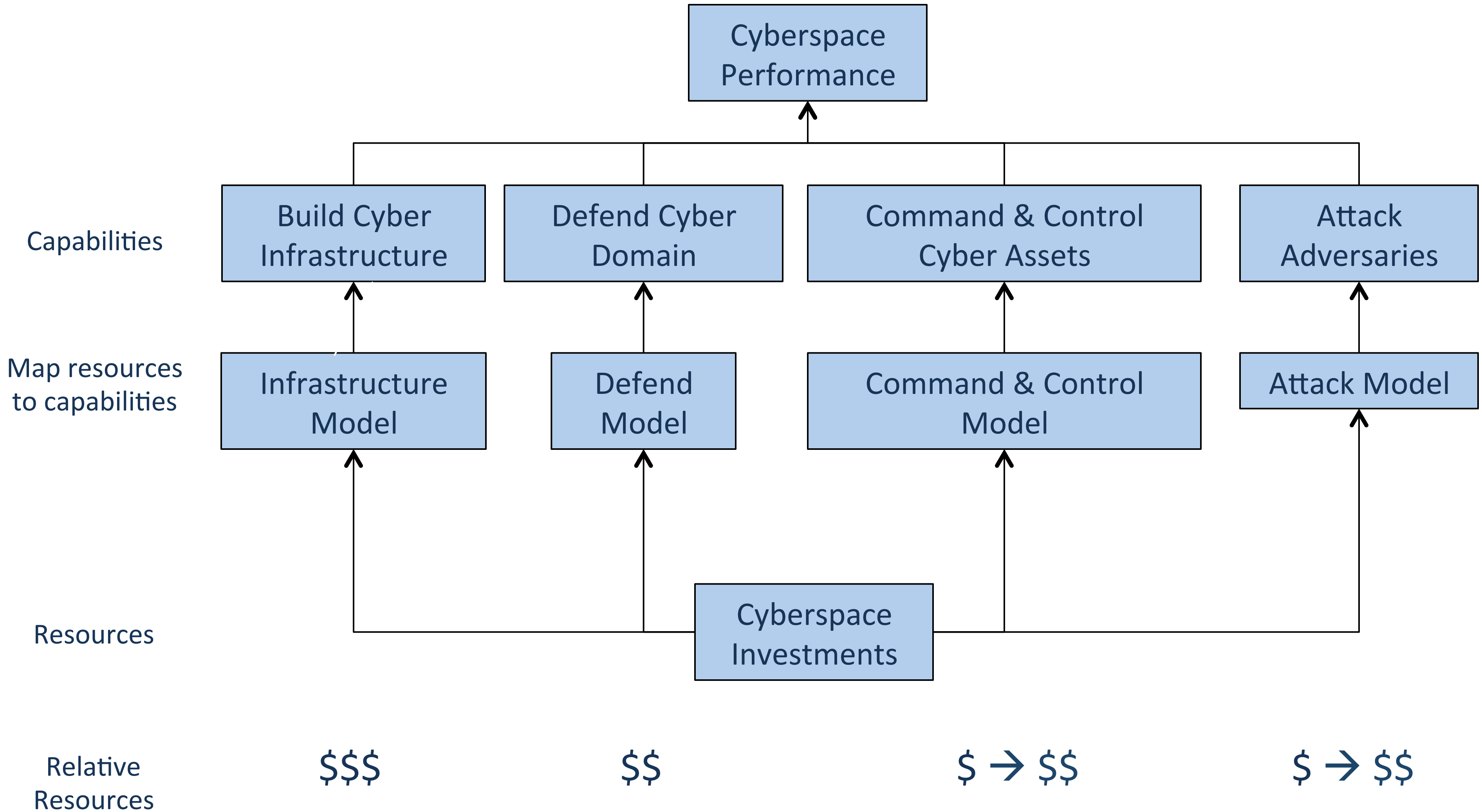
- Future architecture implementation
- Future resource execution
- Future cyber attacks
- Future technology revolutions

Key modeling ideas

- Develop cyberspace analytical models
  - Identify fundamental cyberspace functions that underwrite AF capabilities
    - Use verb and object
    - Map to other frameworks as required
  - Use analytic models to map resources to capabilities
    - Capture the fundamental structure of each capability
- Integrate into Air Force Space Command Investment Planning Process analysis tools
  - Decision analysis
  - Optimization



Cyberspace Model Concept



Build Cyber Infrastructure

Capability to provide operations, maintenance, and modernization of the Cyberspace Infrastructure on both classified and unclassified Air Force networks.

This includes requirements specification, design, procurement, facilities (power, cooling, and security), unit testing, integration and system testing, manpower, administration, and system technical support for hardware, software, and communications.

- Classified networks
  - Operations
  - Hardware
  - Communications
  - Applications
    - Mission
    - Business
- Unclassified networks
  - Operations
  - Hardware
  - Communications
  - Applications
    - Mission
    - Business

Trends

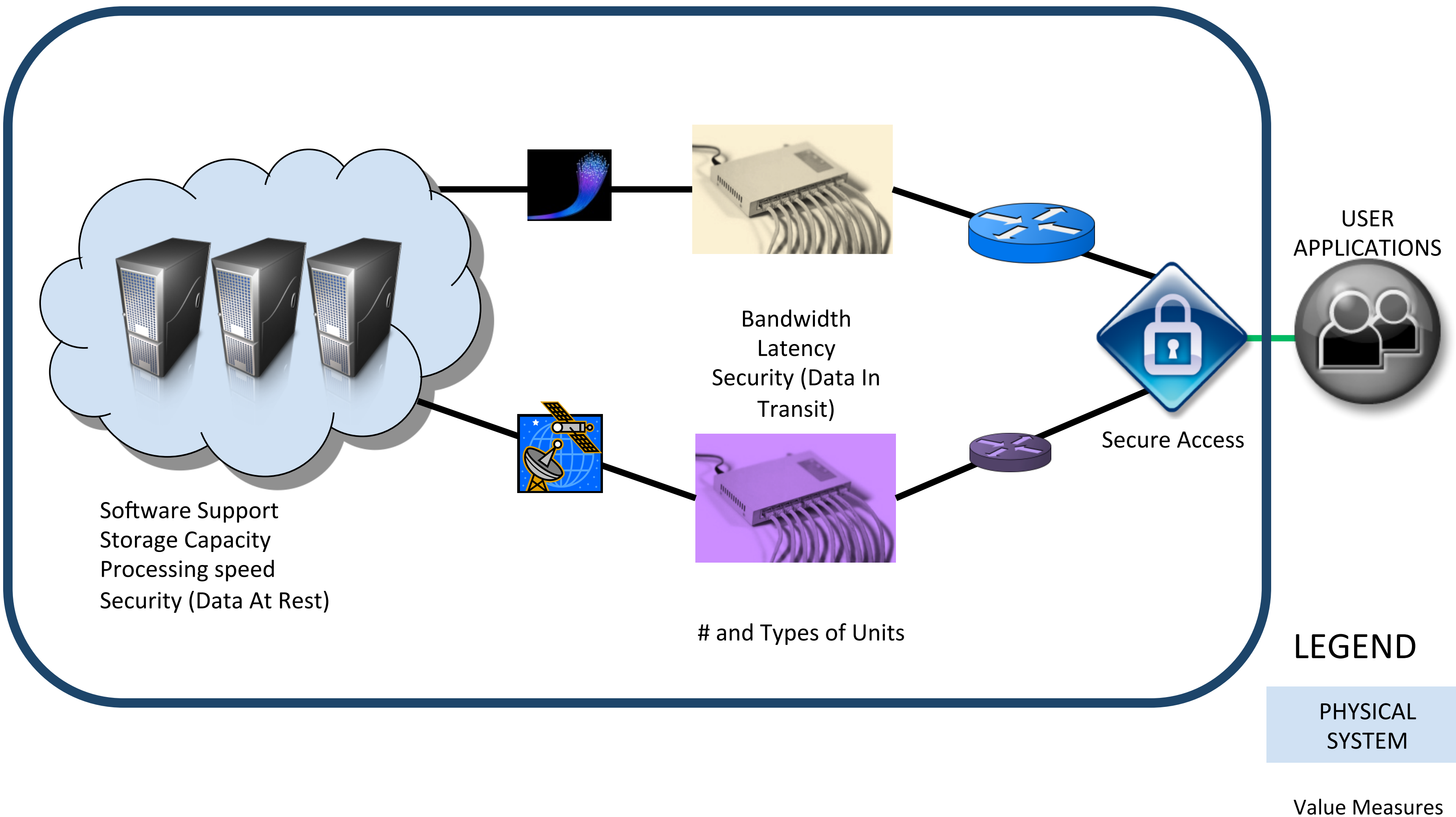
Operational
- ↑ interconnected systems
- ↑ media
- ↑ data
- ↑ bandwidth
- User (mobile, more/shorter messages)

Technology
- Service architectures
- Big Data
- Virtualization
- Clouds

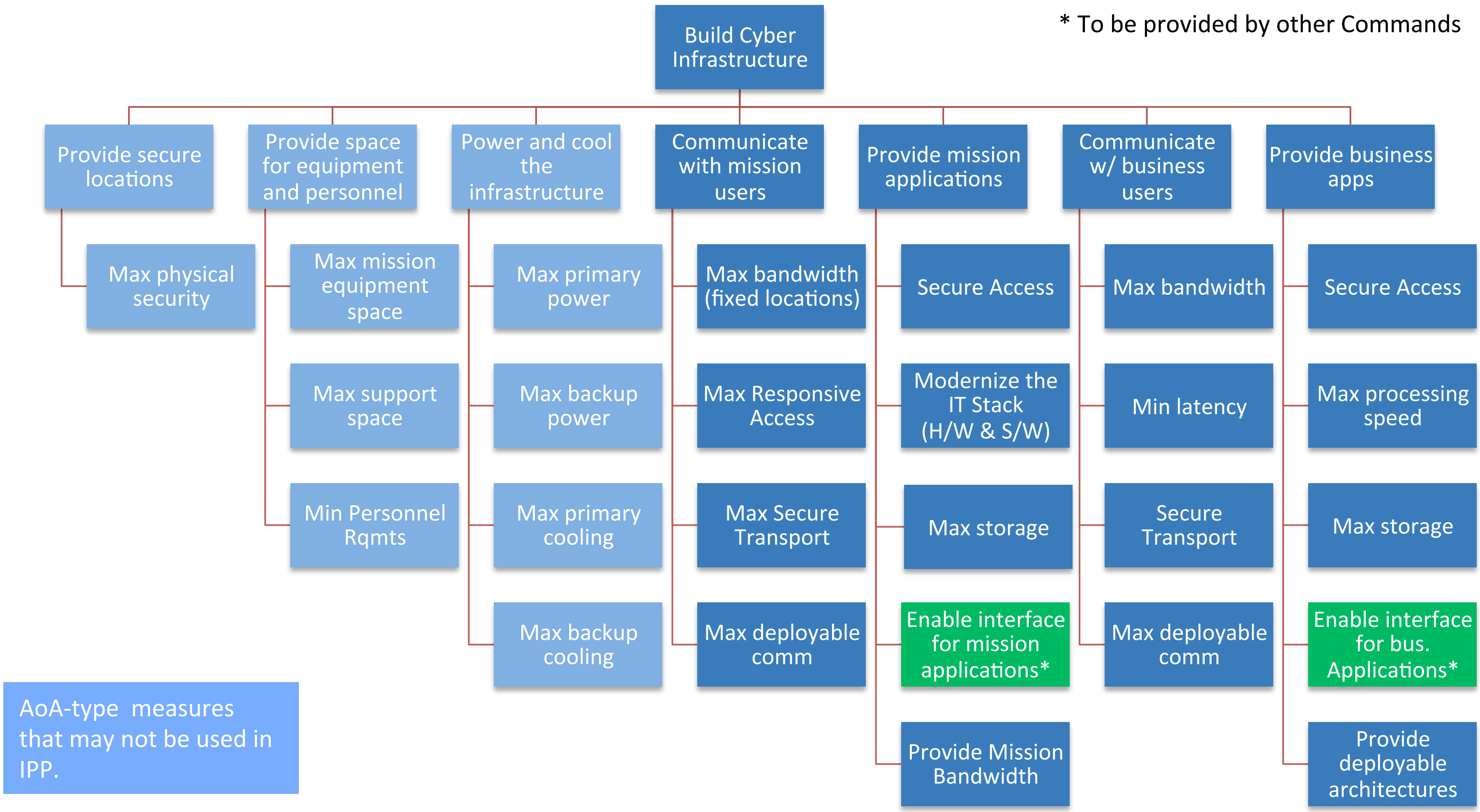
Hardware
- ↓ size
- ↑ power
- ↑ cooling

Software
- ↑ applications

Conceptual Cyber Architecture and Value Measures



Build Cyber Architecture
Functional Architecture Value Model

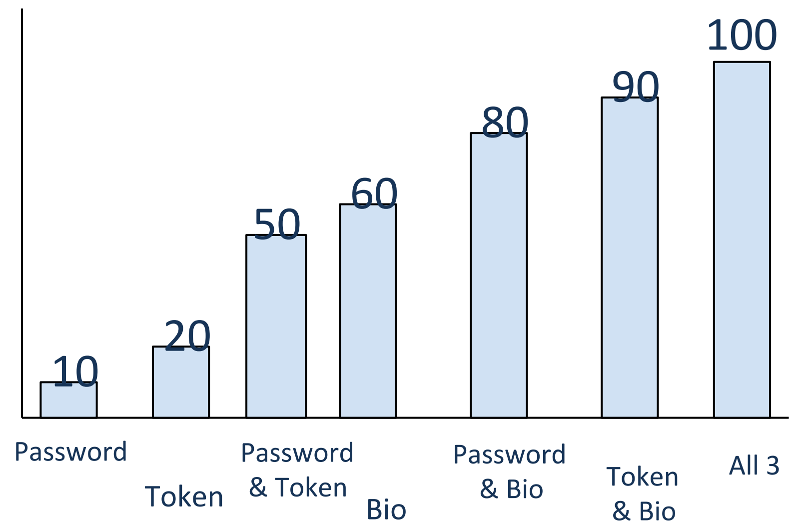


Modified from illustrative example in Parnell, G., Bresnick, Johnson, E., & Tani, S., Decision Analysis Handbook, OR/MS Handbook Series, Wiley & Sons, 2013

Provide Secure Access

- Secure access depends on
  - Something you have → token, CAC
  - Something you know → password, PIN
  - Something you are → biometrics

- Risk assessment
  - Failure = Highest risk
  - Just P/W = Significant risk
  - P/W & Token = Moderate risk
  - Token & Bio = Low risk
  - All three = Lowest risk



Example of discrete value measure.

Maximize Secure Transport

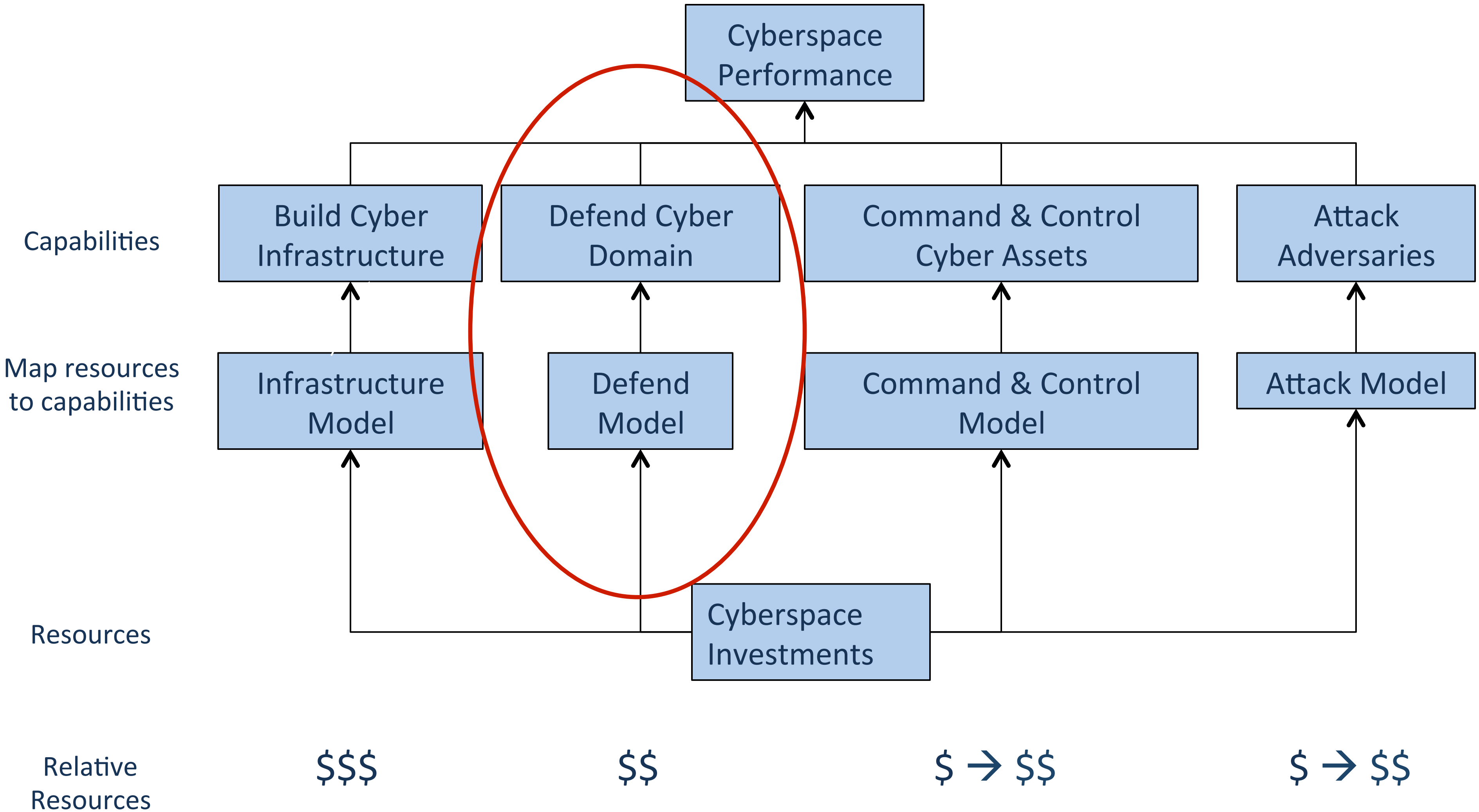
- Transport security depends on hardware and software
  - Built matrix with possible options for hardware and software
  - Determine value of each cell of matrix
- Definitions:
  - Best Gov't = Nuclear Command and Control
  - Gov't = Identify Friend or Foe
  - Best Com'l = Critical Defense Industrial Base
  - Com'l =Today Small Unmanned Aeronautical Vehicles

Software

Hardware	Best Gov't	Gov't	Best Com'l	Com'l
Best Gov't	100 (LR)	90	75	50
Gov't	95	85	70 (MR)	40
Best Com'l	80	65	50 (SR)	20
Com'l	70 (MR)	60	30	0 (HR)

Example of a two dimension value measure using risk HQ USAF assessments .

Cyberspace Model Concept



Defend Cyber Domain

Defend capabilities

- Prevent
- Detect
- Respond (and recover)

Capability Measures

- *Confidentiality*: info not disclosed to unauthorized parties
- *Integrity*: info accurate/complete and not modified
- *Availability*: info available to authorized parties

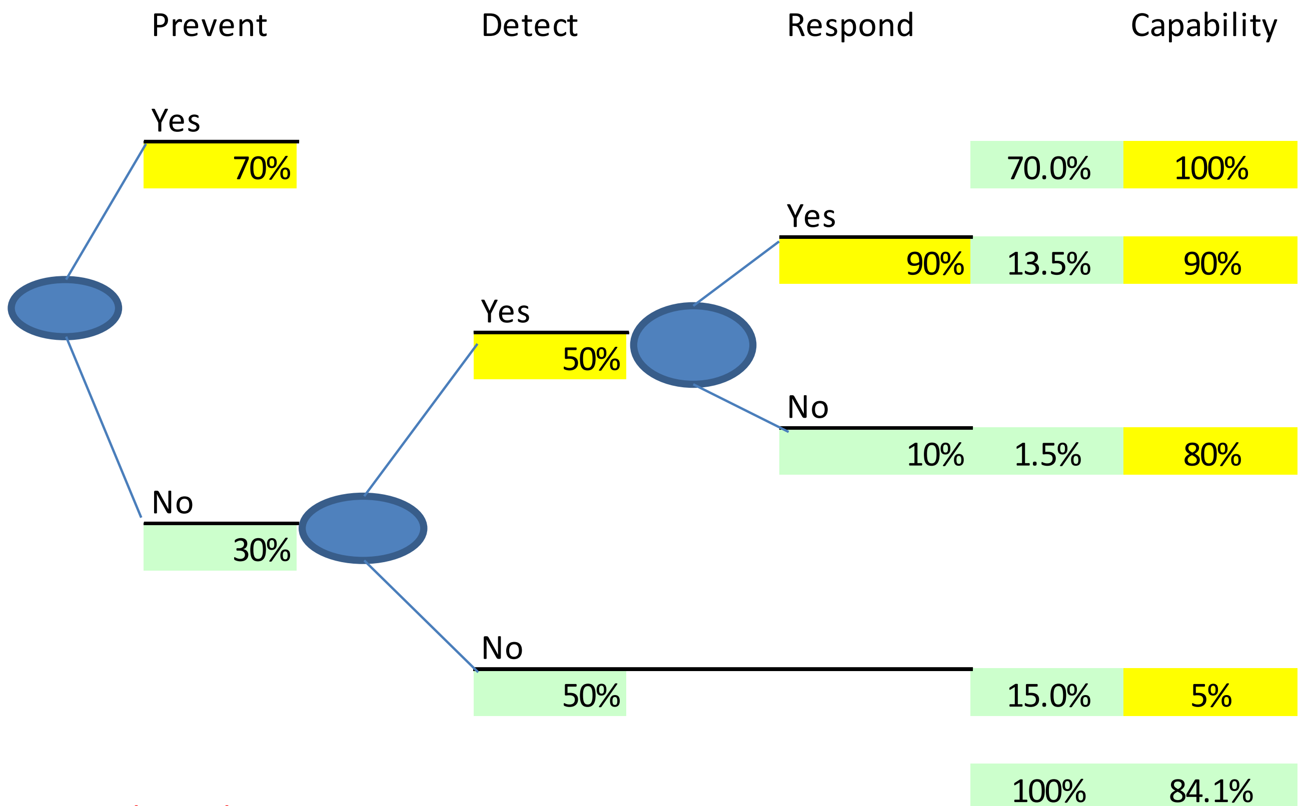
Seven Attack Classes

1. Confidentiality (C) → Joint Strike Fighter data stolen through cyber espionage
2. Integrity (I) → Weather data changed to reflect nonexistent storm
3. Availability (A) → Denial of Service against air mobility web site
4. C & I → Military Deception; espionage + PSYOPs
5. C & A → IADS data viewed & take it down when needed
6. I & A → Modified data used by critical infrastructure before being taken down
7. CIA → Multiple attacks against deployed NIPR Net

Core

Defend Cyber Domain – Model

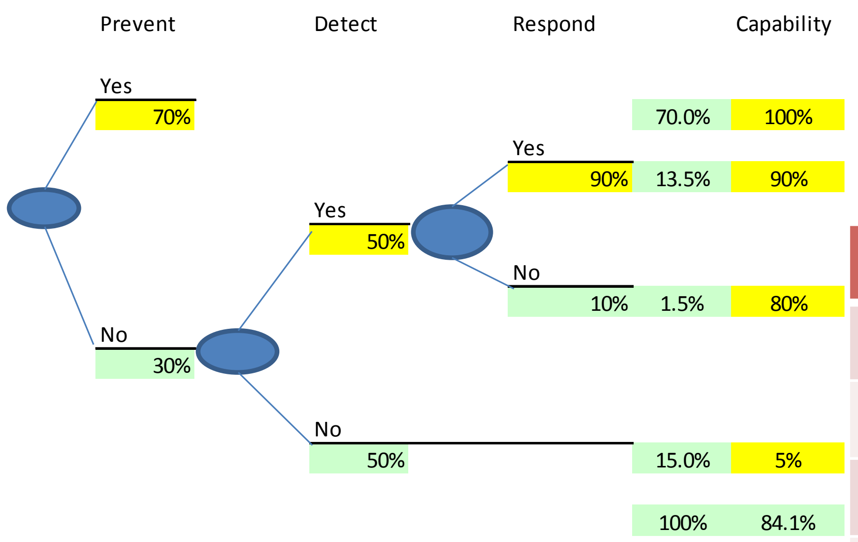
Confidentiiality (C) - JSF data stolen



Notional Numbers

Defend Cyber Domain Scoring Methodology

Confidentiiality (C) - JSF data stolen



Confidentiality	Prevent	Detect	Respond
Baseline	0.15	0.25	0.3
System 1	Low	Med	Low
System 2	Low	Low	Low
System 3	Low	Low	High
Package 1	0.5	0.7	0.6
System 1+	Med	Med	Med
System 2+	Low	High	Med
System 3++	Med	Med	Low
System 4	Low	Low	Low

Defend Cyber Model before and after COAs

Baseline

Cyber intrusion event	Conditional Probability: Prevent	Detect	Respond	Proabability of Mission Assurance	Probabilty of Mission Risk
Confidentiiality (C) - JSF data stolen	70%	50%	90.0%	84.1%	15.9%
Integrity (I) - Weather data shows nonexistent storm	80%	70%	70.0%	92.5%	7.5%
Availability (A) - Denial of service on mobility website	10%	90%	50.0%	79.3%	20.7%
C & A: IADS data viewed and taken down when needed	80%	80%	50.0%	93.8%	6.2%
C I A : Multiple attacks on deployed SIPRNet	90%	90%	90.0%	98.1%	1.9%
			Average	89.5%	10.5%
			Minumum	79.3%	20.7%

Baseline with funded COAs

Cyber intrusion event	Prevent	Detect	Respond	Proabability of Mission Assurance	Probabilty of Mission Risk
Confidentiiality (C) - JSF data stolen	90%	60%	90.0%	95.5%	4%
Integrity (I) - Weather data shows nonexistent storm	80%	80%	90.0%	94.4%	6%
Availability (A) - Denial of service on mobility website	10%	100%	70.0%	88.3%	12%
C & A: IADS data viewed and taken down when needed	90%	90%	70.0%	97.9%	2%
C I A : Multiple attacks on deployed SIPRNet	95%	100%	90.0%	99.5%	1%
			Average	95.1%	4.9%
			Minumum	88.3%	11.7%

Notional Numbers

Multiple Objective Decision Analysis is used to combine the four models of the Cyber Value Model

Cyberspace Performance

Build Cyber Infrastructure

Communicate with mission users
- Max bandwidth
- Min latency (TBD)
- Secure Transport
- Max deployable comm

Provide mission applications
- Secure Access
- Max processing speed
- Max storage
- Develop and maintain applications
- Provide deployable architectures

Communicate w/ business users
- Max bandwidth
- Min latency
- Secure Transport
- Max deployable comm

Provide business apps
- Secure Access
- Max processing speed
- Max storage
- Develop and maintain applications
- Provide deployable architectures

Defend Cyber Domain

Mission Assurance
- Prevent
- Detect
- Respond

Command & Control Cyber Assets

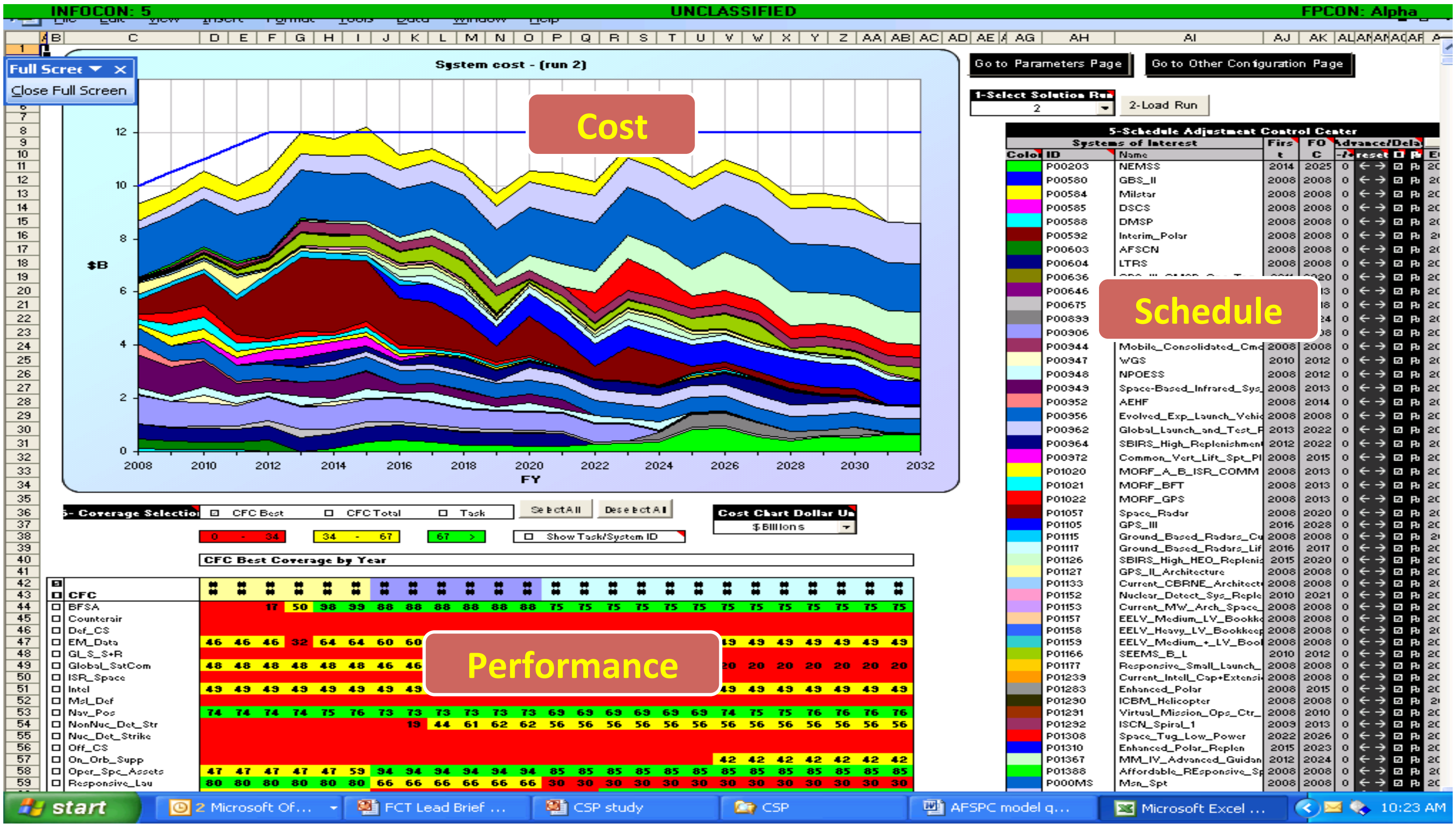
Mission Assurance
- Monitor
- Assess
- Plan
- Execute

Attack Adversaries

Mission Assurance
- Access network
- Access target
- Avoid Detection
- Avoid Attribution
- Execute Mission

IPP uses decision analysis and optimization to analyze performance, cost, and schedule trade offs

Notional data that shows a force mix under the budget.



Air Force Space Command Assessment

- Process:
  - Dr. Parnell facilitated AFSPC A8/9 Planner/Analyst Team resulting in a rough draft of the Cyber models
  - Subject Matter Experts worked with Planner/Analyst Team to refine the models and provide initial assessments
  - SMEs finalized model and assessments as homework and presented conclusions to final working group
  - Senior analysts and stakeholders were briefed on initial results
- Discoveries
  - SMEs quickly grasped the methodology and spent quality time refining the conditional probabilities and assessments vice pondering the methodology
  - Structured risk definitions simplified normalizing the value scores and probability estimates
  - SMEs got new insights on their alternatives and how to improve them

The methodology and results were understandable to SMEs, SHs, and DMs.

References

- Brown G. G., Dell R.F., Holtz H., Newman A.M., (2003) How US Air Force Space Command optimizes long-term investment in space systems. Interfaces 33(4):1-14
- Buckshaw, D. L., Parnell, G. S., Unkenholz, W. L., Parks, D. L., Wallner, J. M. and Saydjari, O. S., *Mission Oriented Risk and Design Analysis of Critical Information Systems*, Military Operations Research, 2005,Vol 10, No 2, pp. 19-38.
- Parnell, G. S., Driscoll, P. J., and Henderson D. L., Editors, Decision Making for Systems Engineering and Management, 2nd Edition, Wiley Series in Systems Engineering, Wiley & Sons Inc., 2011
- Garvey, P. R., Moynihan, R. A., and Servi, L., *A Macro Method for Measuring Economic-Benefit Returns on Cybersecurity Investments: The Table Top Approach*, The MITRE Corporation, 1 November, 2011
- Parnell, G. S., *Value-Focused Thinking Using Multiple Objective Decision Analysis*, Methods for Conducting Military Operational Analysis: Military Operations Research Society, Editors, A. Loerch & L. Rainey, 2007, pp. 619-656
- Burk, R. and Parnell, G., Chapter 14, *Portfolio Decision Analysis – Lessons from Military Applications*, Advances in Portfolio Decision Analysis Methods for Improved Resource Allocation, Salo, A., Keisler, J., and Morton, A., Editors, Springer's International Series in Operations Research and Management Science, 2011, pp. 333-358.