Strategic Observations and Thoughts on a System Model for Security Metrics/Measurements

Why can't we get traction?

Dr Greg Larsen

Agenda

- Overview…
- …Problem Indicators…
- …An Approach…
- …Some Thoughts to Construct them by…
- …Some Parting Thoughts on focus and priority

Overview

- Security ***ISN'T*** tack-on, add-on, applique' or a subordinate feature of nets, systems, or components!
  - It is an integral feature of a capability - not separable from the whole
- Getting the metrics right means making security more than just a measurement in the supply chain and instead an ***integral part*** of the larger business equation that represents the entirety of dimensions that result in progressive security improvement!
- ***Key words***: efficacy, affordability, satisfaction, expectation, performance, alignment, adjudication
  - Words that have meaning to both user/consumer and provider/performer
    - Ie demand/supply and demand/supply environments
- *Perhaps* we need a system model for security metrics/measures that enables a holistic and multiple but consistent views of security -- a new or enlarged synthesis of security evaluation frameworks, methods, and analytics
  - NIAP/CC, T&E, M&S, SE, OR…etc

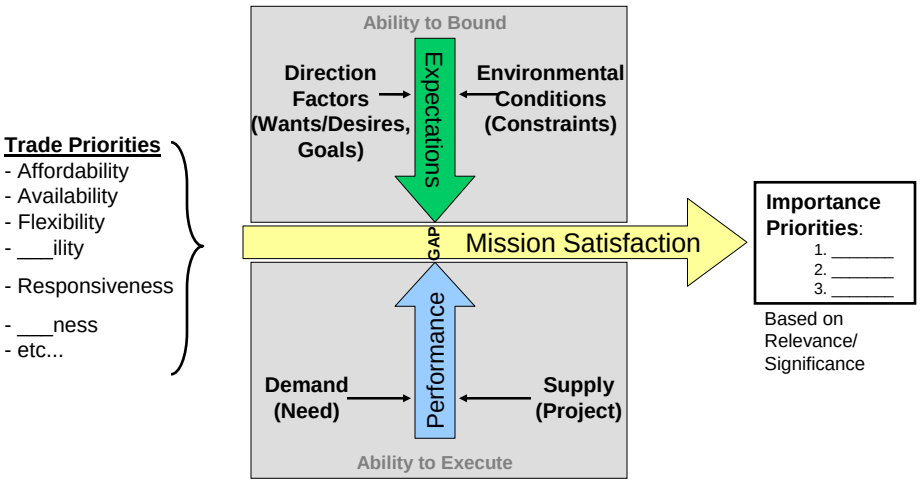
2

Some Questions

- What do we measure that's **valuable** to the consumer/user of security from which demands arise or should arise? … and useful to providers
- How would we observe **satisfaction**? … from both sides and to adjudicators
  - Expectations measurement minus Performance measurement?
- What do we analyze that allows comparative **alignment** of "demands" with "supplies"? … in order to make trade-offs
  - Product/service
  - Process/procedure
  - Control/influence
  - System/net
- How do we obtain a **balance** between demand-side measurement and supply side measurement and expose (make explicit) the measurement of synthesis and integration contributions? … to judge the quality of decisions
- **Adjudication** begins with the business equation and the relative trade-offs of features; one of which is security

3

Conceptual Metrics/Measures Data Model

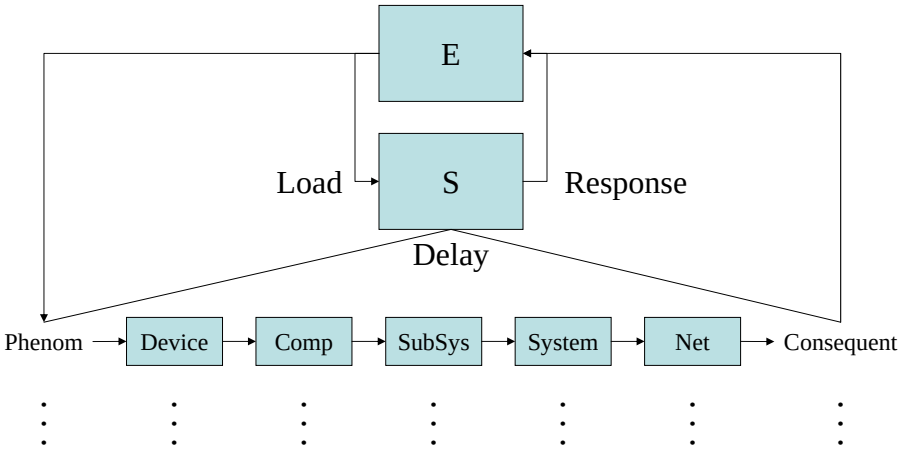


All four quadrants are expressed as situation, task, asset

Need: **feasibly achievable expectation**
Project: **executable work package to satisfy a need**

4

A 2-body System Model



Asset Types block: **HW/SW/People**
Common Functions per block: **ingress, egress, production, controls, I/F**
Dimensionless Parameter per block: **Erlang(s) (rho-R*C*H)**

5

Indicators of a Problem (or issues?)

- Examine metric/measurement efforts of just the last 5-10 years
  - Most "live" in the supply chain view of the world
  - Some "live" at the interface between the supply chain and the demand chain
  - Almost none are meaningful outside the developer/provider community OR are so low in fidelity or hyper-context sensitive to be of little value to users/consumers or authorities responsible for adjudication/alignment of demands for supply of security
  - Few are measurement in the NIST engineering meaning of measurement
    - Every measurement is specified with an associated uncertainty
    - Measurements can be used to derive higher level indicators
    - Uncertainty Analysis Methods not well known or applied to system ***security assurance***
- Assuming metrics are sufficient (I contend NOT),
  - How many do we (whose we) really need just to characterize the value/cost of the supply of security?
  - What are we really measuring?
    - Product or service
    - Process or procedure
    - System or net
    - Controls or influence

6

More indicators of problem(s)

- What is the character of the assets that we are measuring and do they make a difference?
  - HW measures
  - SW measures
  - System measures
  - Net measures
  - Integration measures
  - Capability measures
- Business Models for categories of security implementing assets
  - HW, SW, Systems, Missions

7

Asset Category Business Model Variation

- Asset Category Business Model Variation
  - Variations affect metrics/measures choices
    - HW <-- hold production complexity relatively constant <-- gain performance from production experience <-- liability substantially belongs to producer
    - SW <-- increase performance complexity <-- gain price from performance experience <-- liability substantially belongs to buyer
    - System <-- hide complexity <-- gain from integration experience <-- liability usually shared by producer/buyer
  - Net-net
    - HW investment and performance targets "crisp" and risk-taking economically well-disciplined
    - SW investment and performance targets "fuzzy" and risk-taking not economically well-disciplined
    - System investment and performance targets risk averse and risk assessment substitutes for risk management

8

My View of the Problem

- Security capability is measured by its ***absence*** (prevent) AND the ***confidence that*** one will withstand or survive the consequences of security incidents, ie failure to R^5
  - Resist, Recognize, Respond, Recover, Reconstitute
- Using supply-side metrics/measures provides little confidence of value to most consumers of security
  - Prevention is unprovable and requires trust by the user/consumer; however wise the investment and often leads to dissatisfaction or total inability to craft a pragmatic expectation of the security value proposition
  - Consequences can be demonstrated, tested, and evaluated AND their aftermath can be observed and the results of a response judged for all parties involved (demand, supply, integration)

9

An Approach

- A system model for security metrics
- Business system Approach (with caveats)
  - Capability (Performance) / Cost (Price) Curves
  - Features, Characteristics, Factors
    - Of product
    - Of process
    - Of comparative alignment, synthesis and integration
  - Premise: Accumulated experience has two primary effects
    - Cost of production tends to drop with experience (economies of scale and learning curves)
    - Builds new capabilities by improving existing capabilities or development of alternatives (advance of S&T and innovation)

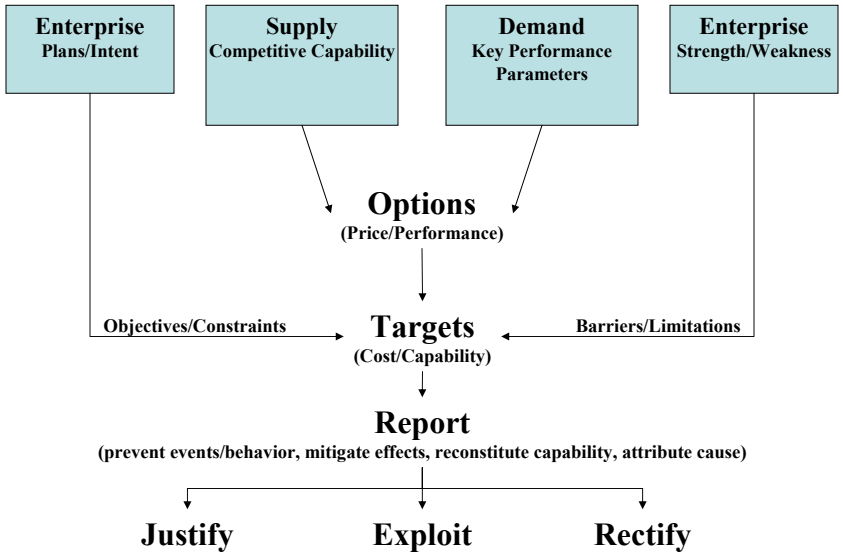
10

Business System Approach

- Business Case can be a system model
  - About where in the Price/Performance (P/P) domain one is operating and where one desires to position to operate.
  - Each "point" represents a composite package of lower dimensional metrics/measures with associated error bounds
- This informs:
  - Strategies that specify what direction, how, and when to change position in this domain
  - Investments that enable and allow change in this domain
  - Priorities that reconcile differences between strategic needs and resource limitations to an accepted level of risk
- A roadmap is the result that expresses implementation of strategy in terms of changes in policies, programs, and resource allocations that execute to achieve the desired operating position

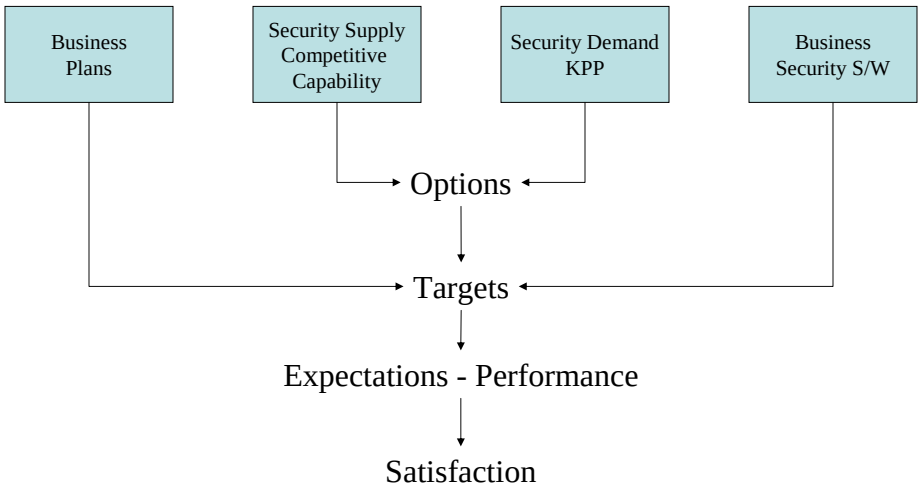
11

Business Case Model



12

Security Version



13

Some Recent Contributions

- Security Measurement - PSM Safety and Security TWG
  - Great start, but… it assumes the business case is adequately and properly articulated with its own set of metrics and measures
- Threat-based Risk Management Methodology - JHU/DoD study of foreign influence on Telecommunications Industry
  - Great start on security demand metrics, but… only a smart part of one-half of the business equation
- IA Metrics - DoD; NR-KPP; NCOW-RM
  - Great start, but… it assumes same issue as PSM-TWG and has no data models
- WP - Office of the Chief Engineer; SPAWARS, Charleston
  - Great warfighter scenario driven and technology agnostic approach to a net-centric security characterization, but… again it assumes same issue as others and has no analytics to align and compare the conceptual and logical technical data models to the metrics and measures of a business-case
- Uncertainty Analysis and Parameter Tolerancing - Castrup; 1992-2001+
  - Great analytics, but… nowhere to apply it
- Each is individually a heroic effort for which there is no connective tissue that makes it relevant and significant to the people and organizations that make the adjudication decisions about efficacious demands for security and commitments to supply security affordably

14

A way-ahead

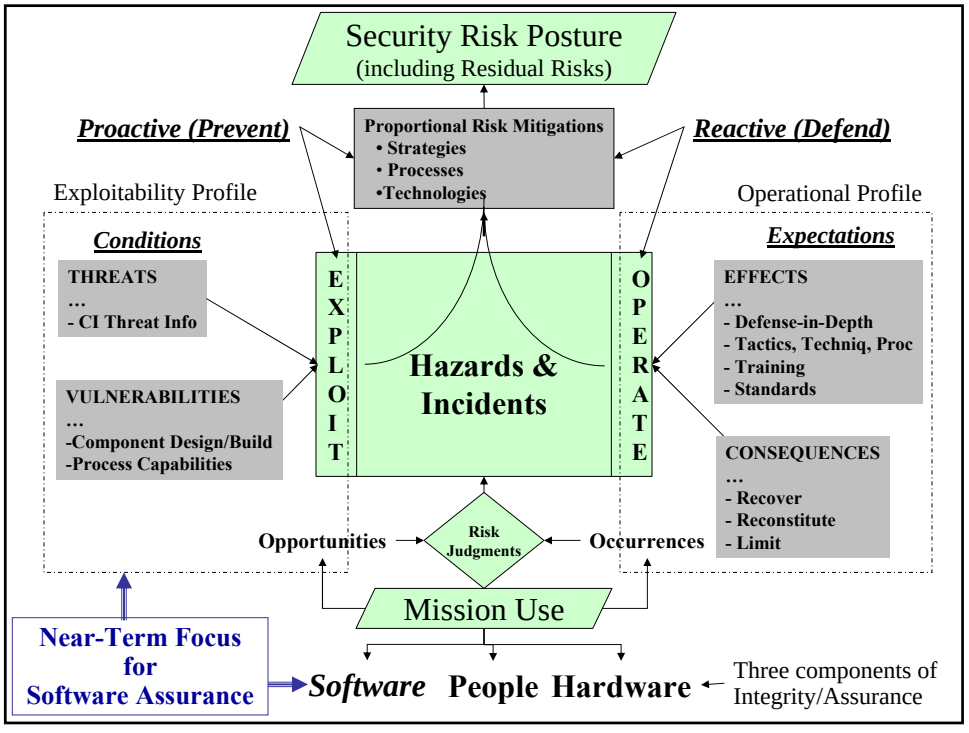
- Problem Definition
  - Define a quantity(s) of interest to ALL parties to the “deal”
- Metrics/Measures Model
  - Develop the Business System equation describing the quantity(s) in terms of measurable variables
- Error Model
  - Develop an error model describing total measurement error as a function of source errors
- Process Error Description
  - Identify process error components for each source and uncertainties
- Uncertainty Model
  - Estimate total uncertainty
- Risk Management
  - Evaluate risks and act appropriately

15

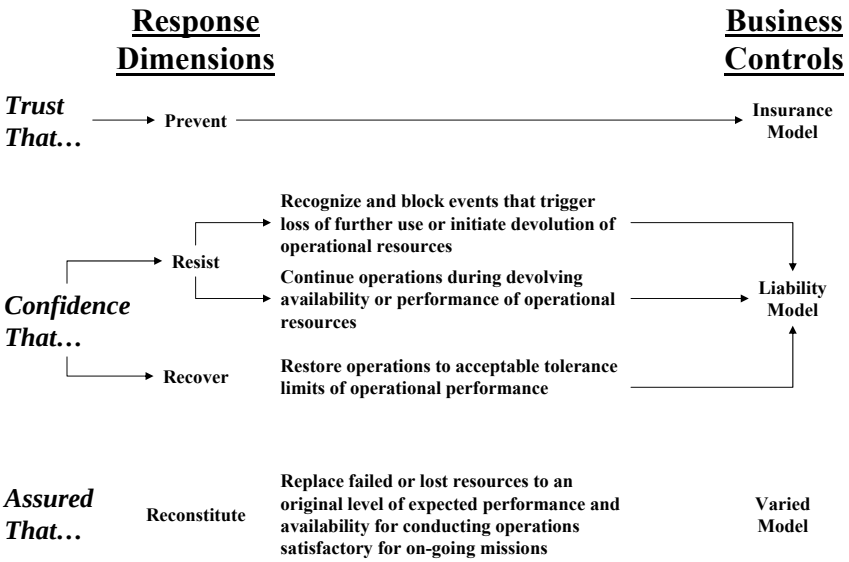
The short-form of the assertion

- Apply what we already know; starting with the simple business case as the problem/system of interest
- Apply known methods to the business model of any "package" of capability (a point in P/P space with associated error bands)
- Make "sense" of as much of the following as possible

16



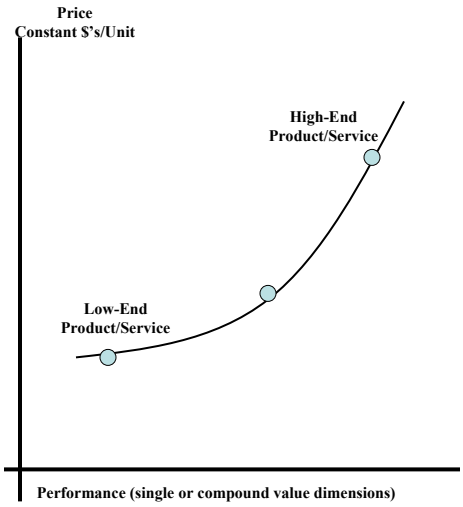
Synthesis of Views



18

Price/Performance Notion

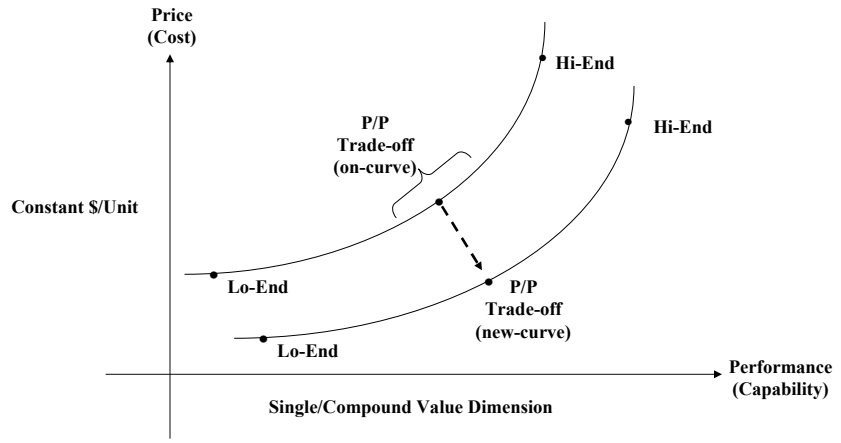
- The relationship between price and the available levels of performance at one point in time. It describes the trade-off between costs and quality
- Trade-off of performance specifications vs. price derived from economic limitations of product and process capabilities



19

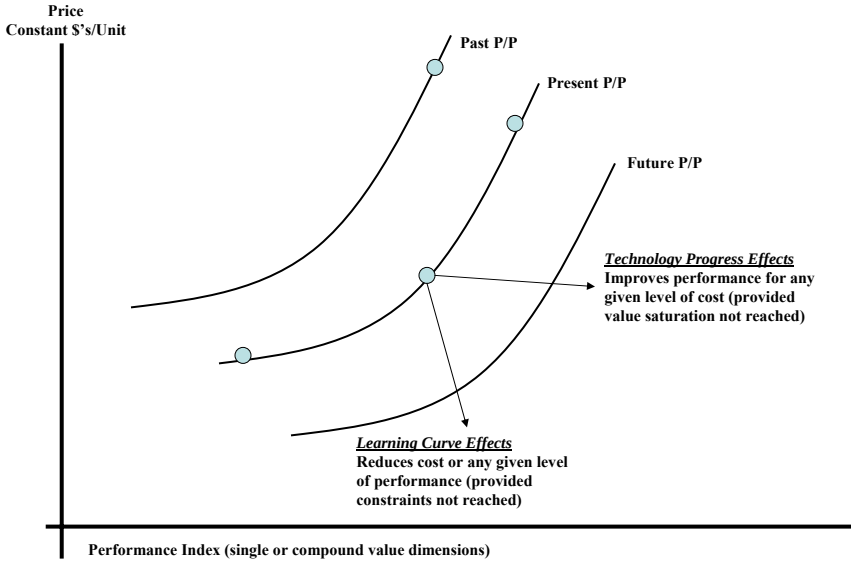
P/P with Experience

(Improve (on-curve) or Fundamental (new-curve)



20

Trends



21

Learning Curves/Technology Progress
What is experience?

- Experience
  - Effects on both costs and capabilities as experience accumulates
  - Generally lowers per/unit costs of production
  - Generally enables capability performance improvements along a profile of the following features constituting a performance "package"
    - Functions
    - Acquisition Costs
    - Ease of Use
    - Operating Costs
    - Reliability
    - Serviceability
    - System Compatibility
- Current operating point in P/P domain is one profile
- Future needs is another operating point in P/P domain

22

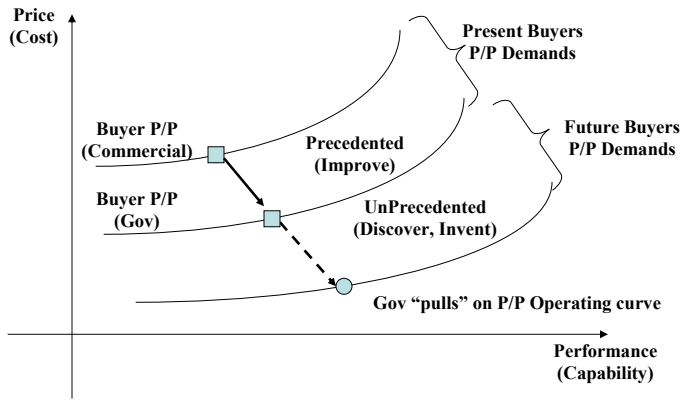
KPP

- General Set
  - Functional Performance
  - Ease-of-Use
  - Reliability
  - Serviceability
  - System Compatibility
  - Operating Cost
  - Acquisition Cost
- Security Specific (Consumer)
  - Conf, Integ, Auth, Avail, Non-Repud
  - Single-Sign-on
  - False Positives
  - Configuration
  - Etc.
  - Expected cost per event
  - Volume, Variety, Velocity
  - TCO
  - Price per "lb of security"

23

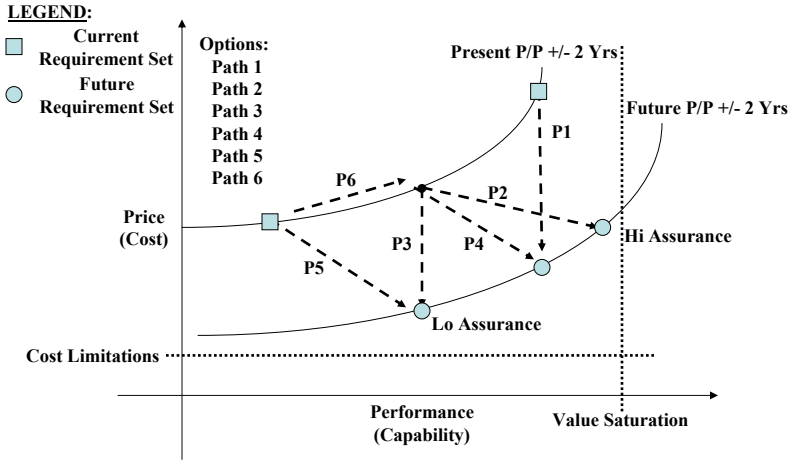
Notion-1

Where are we operating today?



24

Movement Options



Feasibility:
What is feasible near-, mid-, long-term?
What set of requirements does a feasible set represent?
Where are the current requirement sets?

25

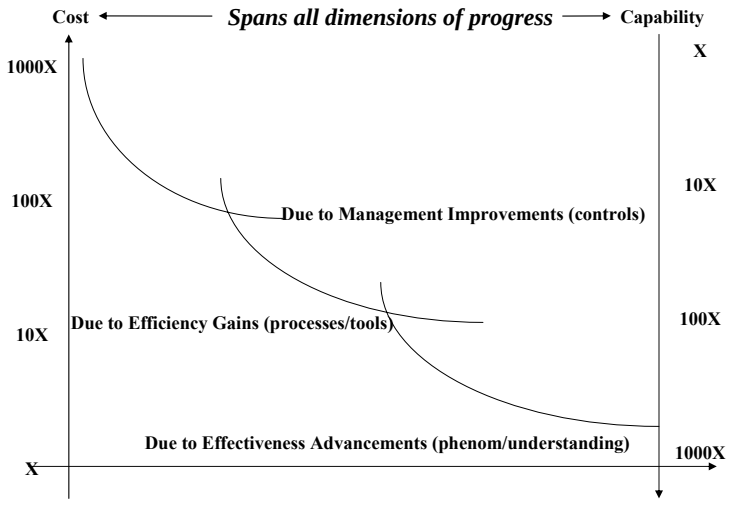
P/P Movement Options

- Invest in order to:
  - Optimize a Figure-of-Merit value to user/customer
  - Optimize position/consolidation of current capabilities
  - Extend position through related capabilities/current K/T
  - Drive process/design K/T to “low cost/hi perf” positions
  - Establish “beachheads” for NEW P/P with NEW K/T
  - Drive NEW P/P positions by “self-cannabalization”
  - Etc.

26

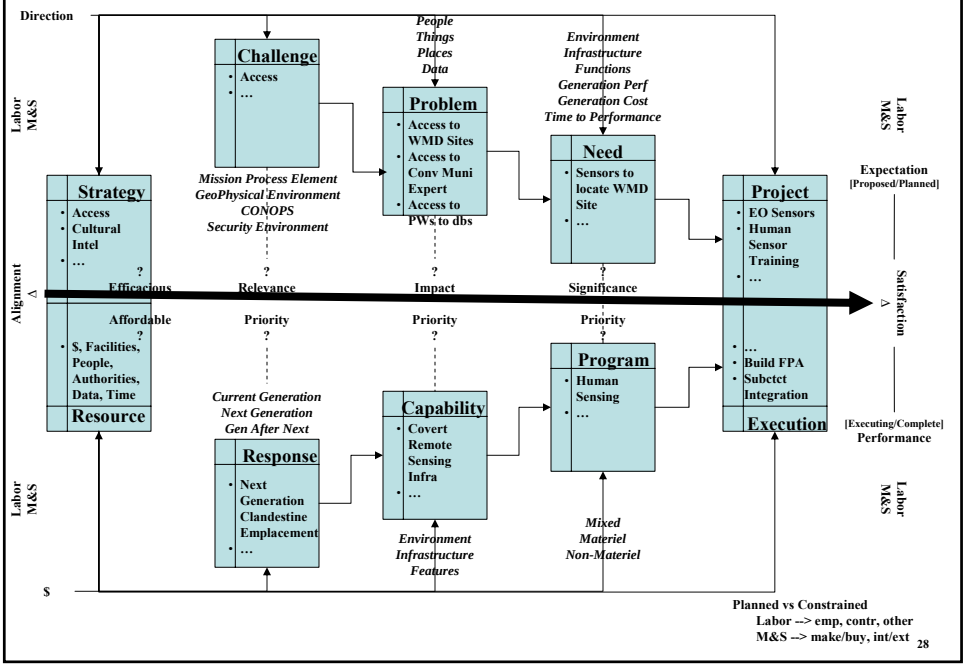
Notional “Package” Figure of Merit

Capability/Cost Ratio

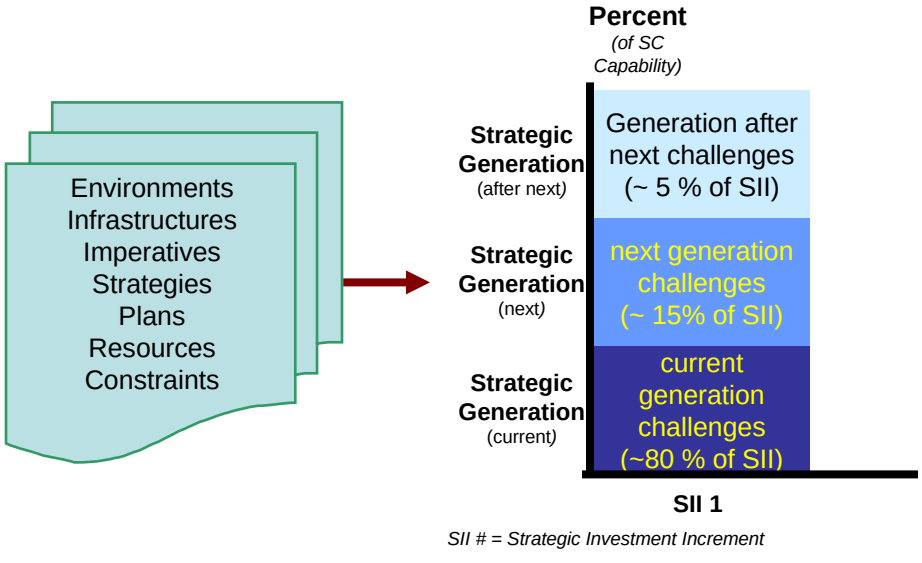


27

Synthesis/Integration Model



From Data to Allocation



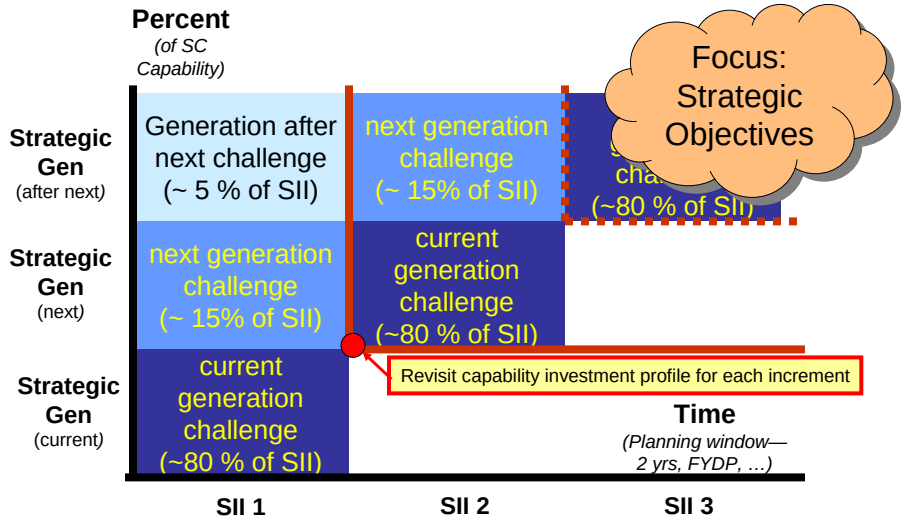
Notional Roadmap

2005 2010 2015 2020

Buy More "Stuff" better	Operate Better Focus: Buy sufficient quantity/capabilities
Engineering Practices Program	Empirical Focus: Best Practices Understanding 25% reduction in program variance through better controls over existing processes
Technology Development Program	Process/Tools Focus: 50 % Improvement Decrease program variance to less than 25% for 90% of programs
Basic Research Program	Phenom/Understanding Focus: 200% Productivity Improvements Repeatedly engineer software intensive systems predicting product quality, performance, schedule and cost within 10%

30

Framework for Tackling the Strategic Challenges



SII # = Strategic Investment Increment

P/P Improvement

How will you satisfy priorities?

Change	Actions	Choice
Policy	List of possibilities	Selection of primary recommendation
Program	List of possibilities	Selection of primary recommendation
Resource	List of possibilities	Selection of primary recommendation

32

Key Words

- efficacy n: capacity or power to produce a desired effect
  - Definition: capability
  - Synonyms: ability, adequacy, capableness, capacity, competence, effect, effectiveness, efficaciousness, efficiency, energy, force, influence, performance, potency, power, productiveness, strength, success, sufficiency, use, vigor, virtue, weight
- afford v: 1: be able to spare or give up; 2: be the cause or source of; 3: have the financial means to do something or buy something; 4: afford access to
  - Definition: able
  - Synonyms: allow, bear, incur, manage, spare, stand, support, sustain
- adjudication n : the act of pronouncing judgment based on the evidence presented
  - v: 2: bring to an end; settle conclusively
  - Definition: judging
  - Synonyms: adjudge, arbitrate, decide, determine, mediate, referee, settle, umpire
  - Antonyms: defer, ignore, not judge

33

Back-Ups

34

Notions

- Notion-1: Price Performance Trades
- Notion-2: Learning Curves vs S&T Advance
- Notion-3: Key-Performance-Parameters
- Notion-4: Security KPP
- Notion-5: NIST Reference on constants, units, and uncertainty

35

Security Profiling

- Identification of Key Performance Parameters (KPP)
- Competitive Rating

36

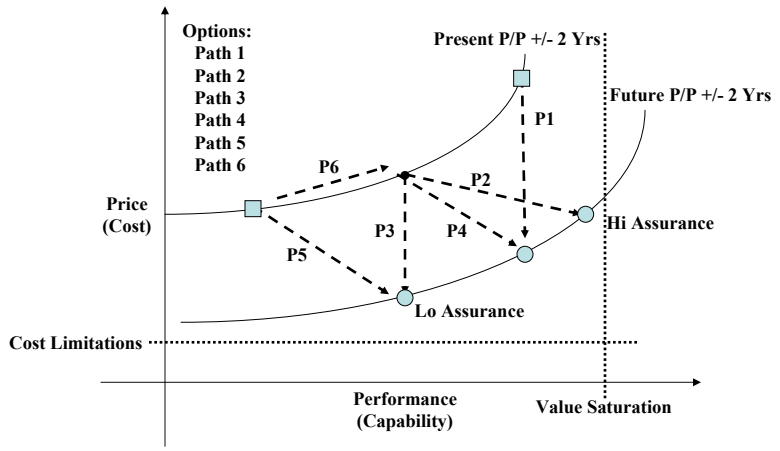
Notion-3

What does history, current practice, future demonstrate?

- Historical Example; utter failure from lack of knowledge, capability, or affordability
  - Trusted Computing
- Current Practices; produces higher priced, lower performing results at any volume, variety, velocity
  - NIAP/CC, Alternative practices
- Future; demands low price, high performance at any volume, variety, velocity
  - Net-Centric -- secure comms, Proliferating Information sources, Power to the edge, etc.

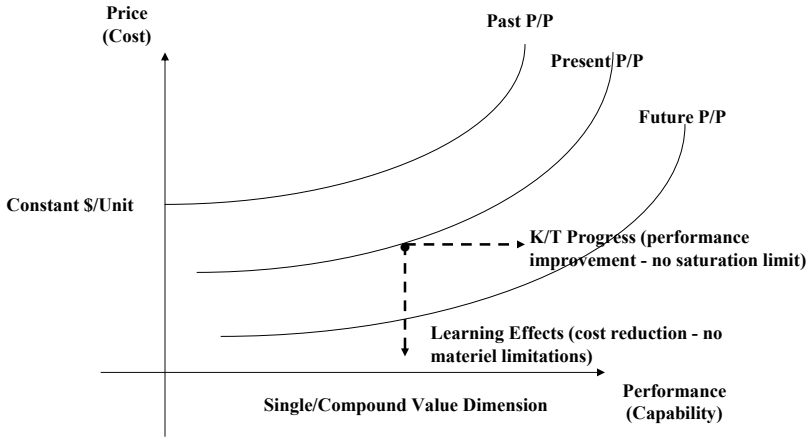
37

Strategy Options



38

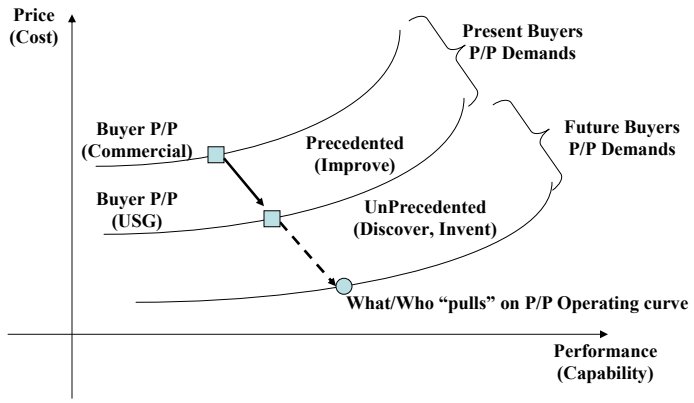
Learning/Progress Effects



39

Notion-2

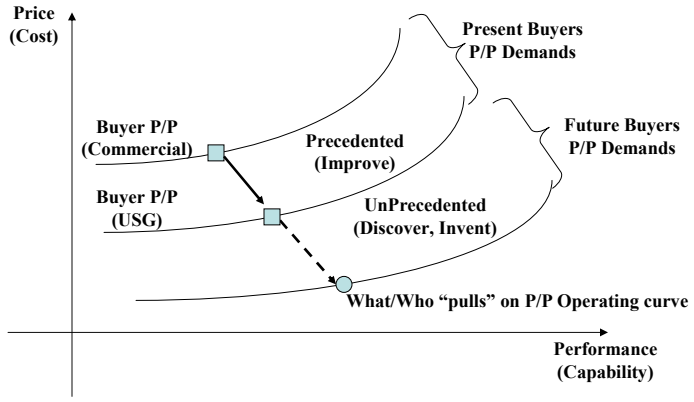
Where are we today?



40

Notion-1

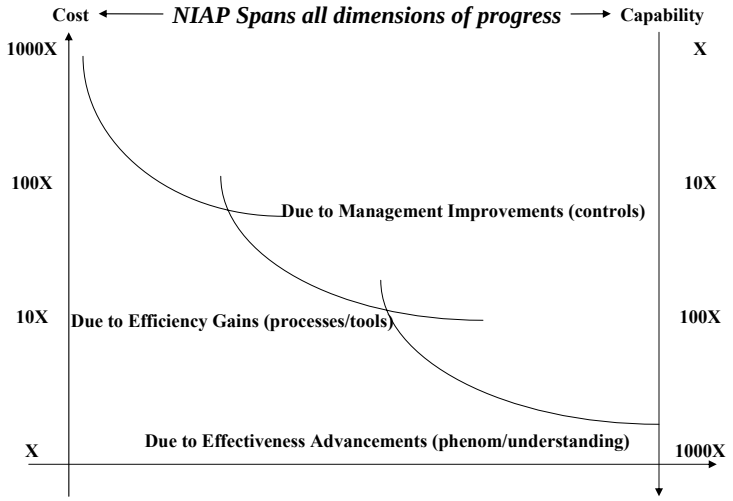
Where is NIAP operating today?



41

Notional "Package" Figure of Merit

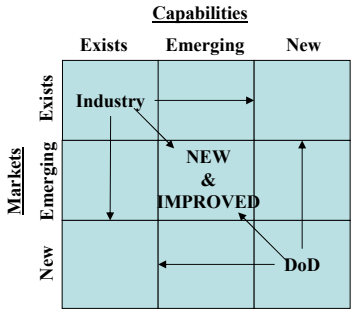
Capability/Cost Ratio



42

Notion-2

What major options address progress?

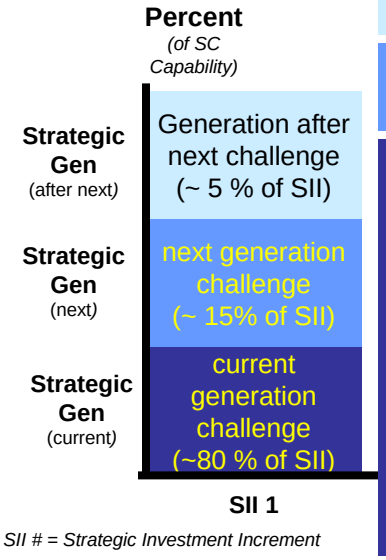


Controls should be improved, efficiencies of processes can be improved, and advances must be made [both the NEW and the IMPROVED require investment]

43

44

Some Sample Capabilities for Strategic Increment #1



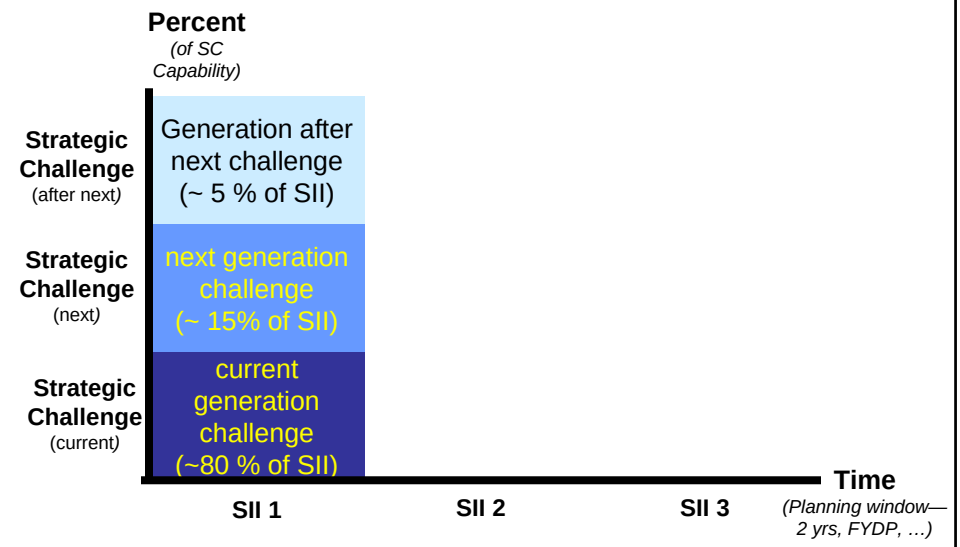
SII # = Strategic Investment Increment

Generation after next challenge:
- Establish IW relationships for preemptive strike
- Integrate human cognition limits into J2-J3 investment

Next generation challenge:
- Intelligence M&S prototype development/experimentation
- Fly-away Joint ISR—how to achieve it without physical collocation

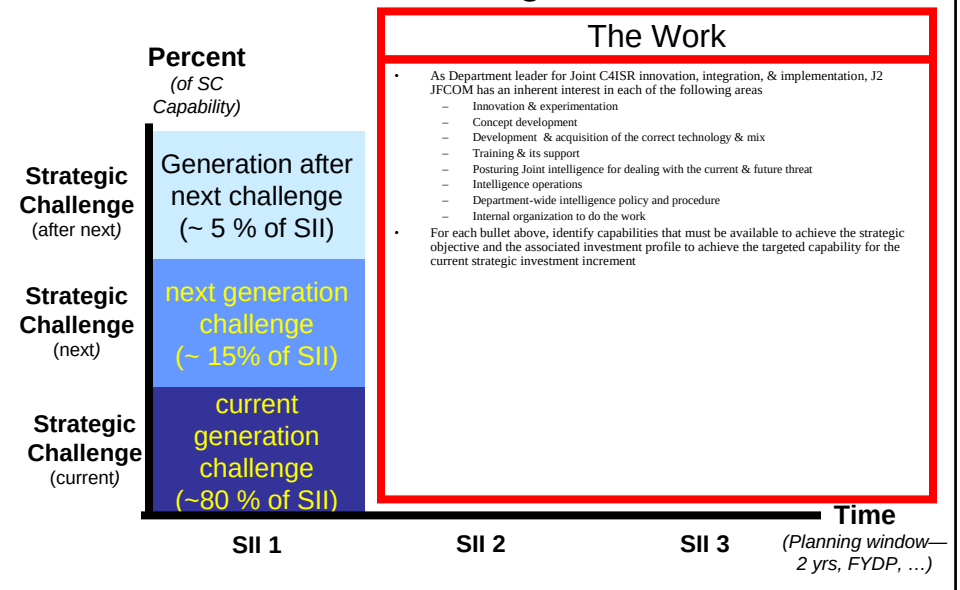
Current generation challenge:
- Common language for Department-wide Joint ISR Products and services that capture decision-makers' real needs/timelines
- Common expression of unmet demands & of levels/types of dissatisfaction
- Identification of tools needed to work integration—disconnects between preceding bullet
- Define data model for integrated Joint C4ISR operations
- Define role in JCIDS
- Reachback that works and can be trusted—CONOPS & experimentation
- Leveraging analysts Department-wide to add value to J2-J3 integrated operations at the effects level
- Conceptual/requirements work for M&S that can drive intelligence play in training—enabling intelligence (payoff/penalty)
- Field experiments to focus on blurring J2-J3 lines
  - The last "12 inches" (machine to commander's head)
  - Allocation of collection capability & ensuring its integration into operations inside adversary OODA loop
  - ISR integration throughout the fires/effects cycle
  - Integration of UAVs into the Joint C2 & ISR
  - Cross-service imagery sharing at tactical echelon
  - Integration of BDA/EA & ISR at effects level

Filling Out the Framework: Focus Now on Strategic Increment #1



SII # = Strategic Investment Increment

Filling Out the Framework: Focus Now on Strategic Increment #1

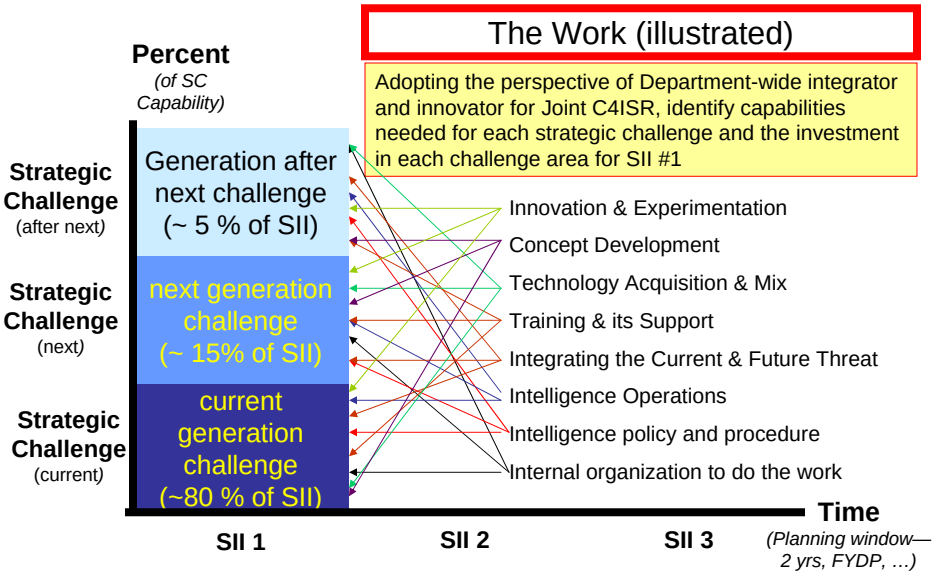


The Work

- As Department leader for Joint C4ISR innovation, integration, & implementation, J2 JFCOM has an inherent interest in each of the following areas
  - Innovation & experimentation
  - Concept development
  - Development & acquisition of the correct technology & mix
  - Training & its support
  - Posturing Joint intelligence for dealing with the current & future threat
  - Intelligence operations
  - Department-wide intelligence policy and procedure
  - Internal organization to do the work
- For each bullet above, identify capabilities that must be available to achieve the strategic objective and the associated investment profile to achieve the targeted capability for the current strategic investment increment

47

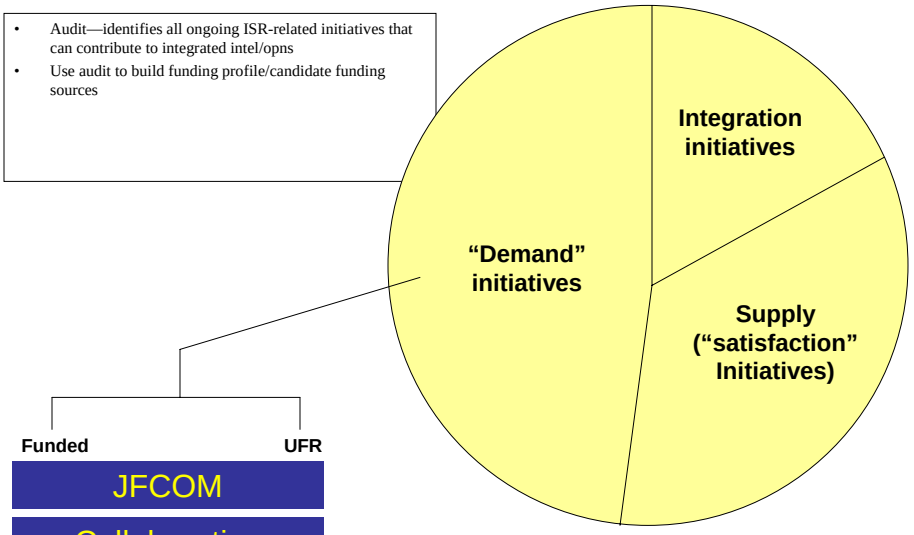
Filling Out the Framework: Focus Now on Strategic Increment #1



48

Developing Funding Estimates

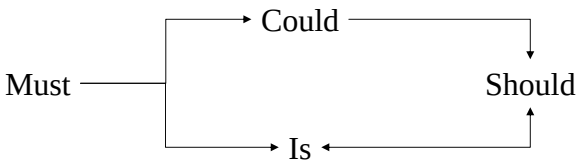
- Audit—identifies all ongoing ISR-related initiatives that can contribute to integrated intel/opns
- Use audit to build funding profile/candidate funding sources



49

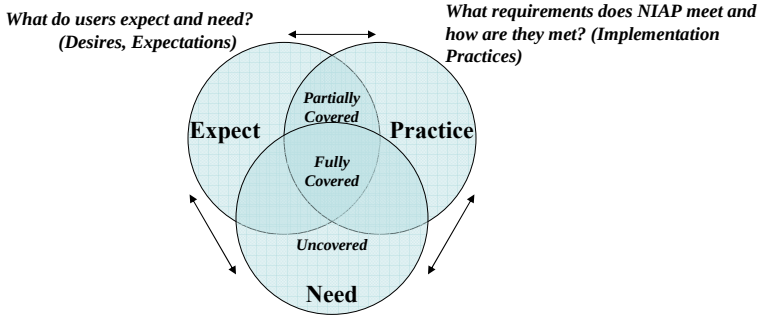
General Structure

- Develop the facts, information, arguments, and recommendations concerning:
  - What must NIAP be? (National policy threshold)
  - What is NIAP? (Experience and fact-finding)
  - What could NIAP be? (Expectation and situation)
  - What should NIAP be? (Analysis and Recommendations)



50

"Requirements" Approach



Without question, priorities and resources determine satisfaction

51

Policy Matrix

- Identified and reviewed 97 policy and legal documents (Over 5000 pages of policy documents) and derived:
  - 201 requirements
  - 56 sets of guidance materials
  - Matrix to follow
- Researched the history of NIAP development
  - Evaluation process and criteria
  - Created a timeline (see chart)

52

Policy Requirements

- Federal Community
  - 31 requirements (IA, Acquisition, Certification & Accreditation, Standards/Guidelines, CIP, & Reporting)
- National Security Community
  - 15 unique requirements (general, Acquisition, Certification & Accreditation, and Reporting)
- DoD
  - 45 unique requirements (IA, Acquisition, CIP, Trusted Computer Systems, Certification & Accreditation, Protection Profiles, and Standards)
- Intelligence Community
  - 2 unique requirements (IA, Certification & Accreditation)
- NIST
  - 13 unique requirements (IA, Standards/Guidelines, Evaluated Products)
- NSA
  - 9 unique requirements (Acquisition, Trusted Computer Systems, Evaluated Products, Protection Profiles)
- NIAP
  - 15 unique requirements (IA)

53