25th anniversary
annual INCOSE
international symposium
Seattle, WA
July 13 - 16, 2015

Adaptive Knowledge Encoding for Agile Cybersecurity Operations

Presenter: Keith D. Willett, CISSP, ISSAP,
PhD Candidate at Stevens Institute of Technology

Agenda

- Bottom Line Up Front (BLUF)
- Problem
- Functional Gap
- Proposed Solution
  - Uniqueness
  - Strategic & Operational Context
  - Solution Overview
    - Cybersecurity Decision Patterns (CDPs)
    - Cybersecurity Decision Pattern Language (CDPL)

BLUF

1. More efficient cybersecurity operations
   - Accelerate processing time
     - Achieve agile cybersecurity operations
2. More efficient training
   - Reduced learning curve
3. Increase explicit organizational knowledge
   - Elicit and codify individual tacit knowledge

Problem Statement

Lack of ability for cybersecurity operations practitioners to *observe*, *orient*, *decide*, *act*, *command*, and *control* within cyber-relevant time to maximize utilization of limited practitioner resources.

We may be doing the right thing, just not fast enough.

Functional Gap

Department of Defense Strategy for Operating in Cyberspace (DSOC)

Active Cyber Defense (ACD) (Current)

- Lead Architect for ACD since its inception
- **ACD Purpose**: integrate, synchronize, and respond within ***cyber-relevant time***[1]
- **ACD Functional Areas**: Sensing, Sense-Making, Decision-Making, Acting, Messaging and Control, ACD Mission Management
- Need for OODA+C2 support for cybersecurity ops practitioners

ACD Reference Architecture (Current)

- Collaboration with Dept of Homeland Security's *Enterprise Automated Security Environment* (EASE)

Cybersecurity Automation (Future)

- **Management**: *making decisions*; logic of governance and adjudication
- **Manipulation**: *taking action*; executing operations; messaging & message set

[1] Journal of Information Warfare, April 2014
Active Cyber Defense: A Vision for Real-Time Cyber Defense
by Michael Herring and Keith D. Willett

Uniqueness of Research 1of3

Cybersecurity Decision Patterns (CDPs)

- Formal knowledge structure
- Minimal content: *context*, *problem*, and *solution*

- *Design Patterns:* codify development knowledge
- *Decision Patterns:* codify operational knowledge

Uniqueness of Research 2of3

Cybersecurity Decision Pattern Language (CDPL)

- Association of CDPs to transcend knowledge and create understanding
- Shared cybersecurity cognitive schema
- Notional Structure: Incident Response Taxonomy
  - Representative workflow
  - Knowledge in context of how practitioners encounter real-world operations

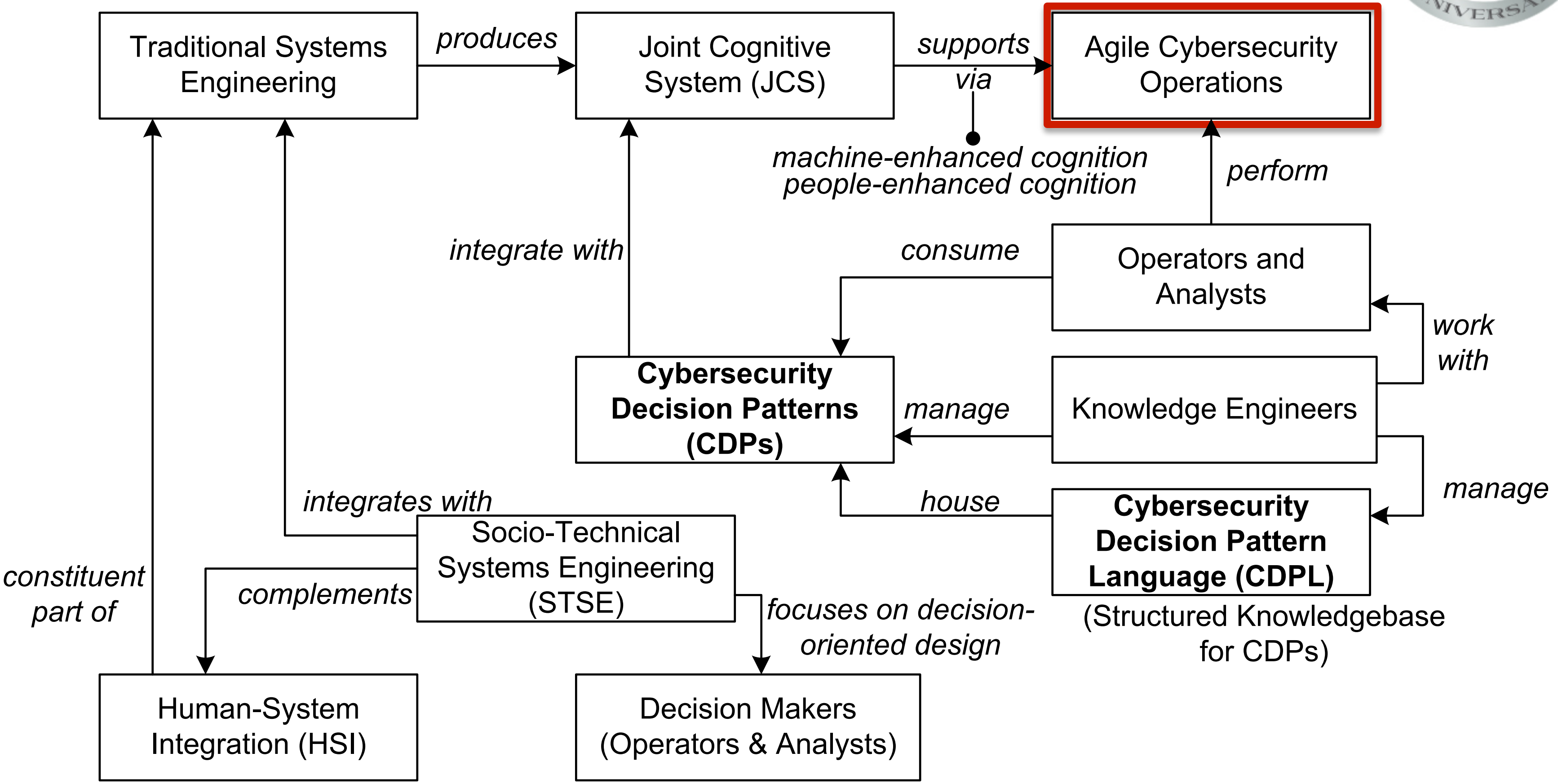
Uniqueness of Research 3of3

Operational Construct for CDPs

- Joint Cognitive System (JCS)
  - Machine-Enhanced Cognition
    - E.g. analytics, decision support system, Bayesian Belief Network, artificial intelligence
  - People-Enhanced Cognition
    - E.g. CDPs and the CDPL

JCS: a system that provides mutualistic symbiosis among humans and machines for cognitive enhancement and continual adaptation in a complex environment

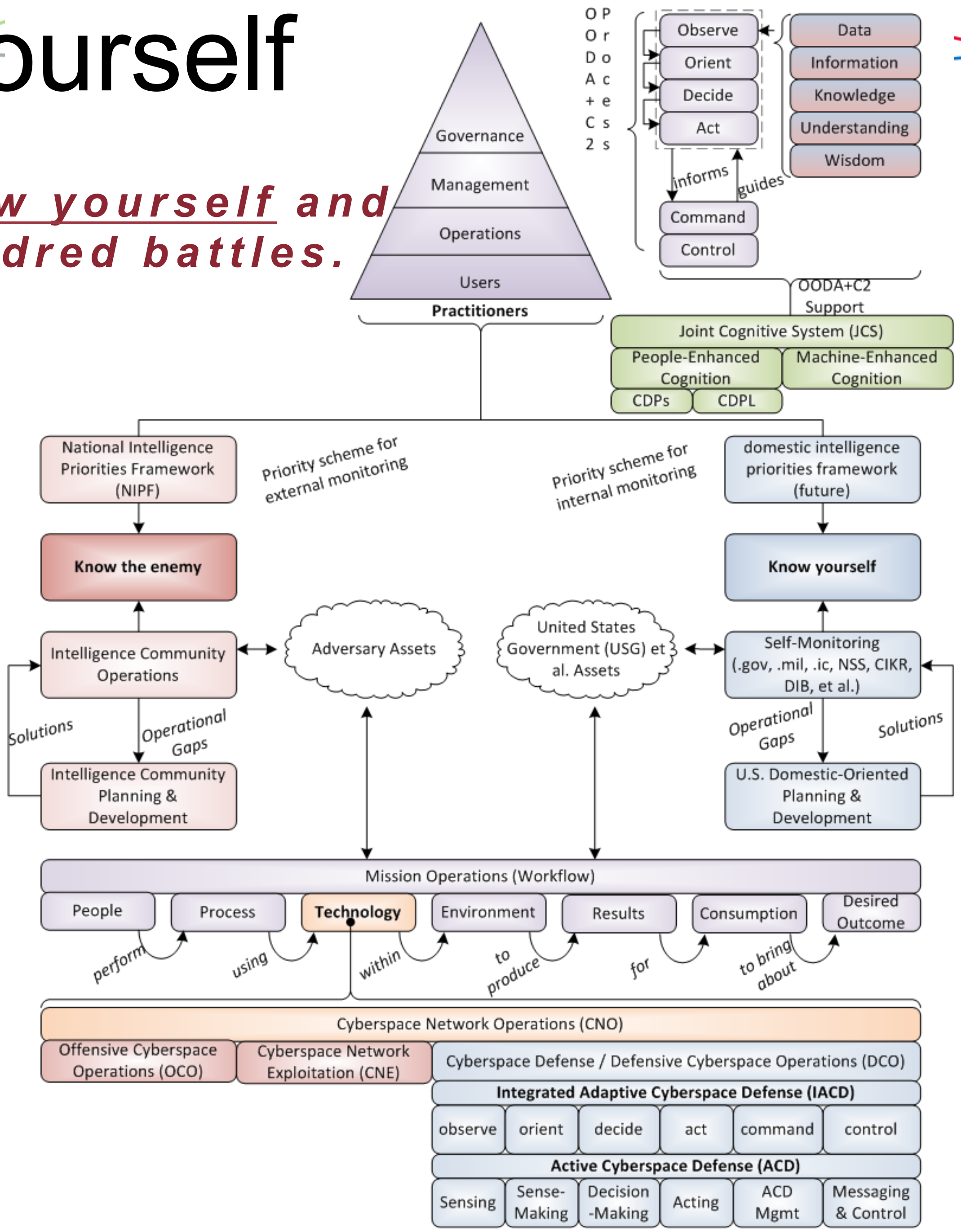
Approach


Traditional Systems Engineering
produces
Joint Cognitive System (JCS)
supports via
Agile Cybersecurity Operations
machine-enhanced cognition
people-enhanced cognition
perform
integrate with
consume
Operators and Analysts
work with
Cybersecurity Decision Patterns (CDPs)
manage
Knowledge Engineers
manage
integrates with
house
Cybersecurity Decision Pattern Language (CDPL)
(Structured Knowledgebase for CDPs)
Socio-Technical Systems Engineering (STSE)
constituent part of
complements
focuses on decision-oriented design
Human-System Integration (HSI)
Decision Makers (Operators & Analysts)

Strategic Context

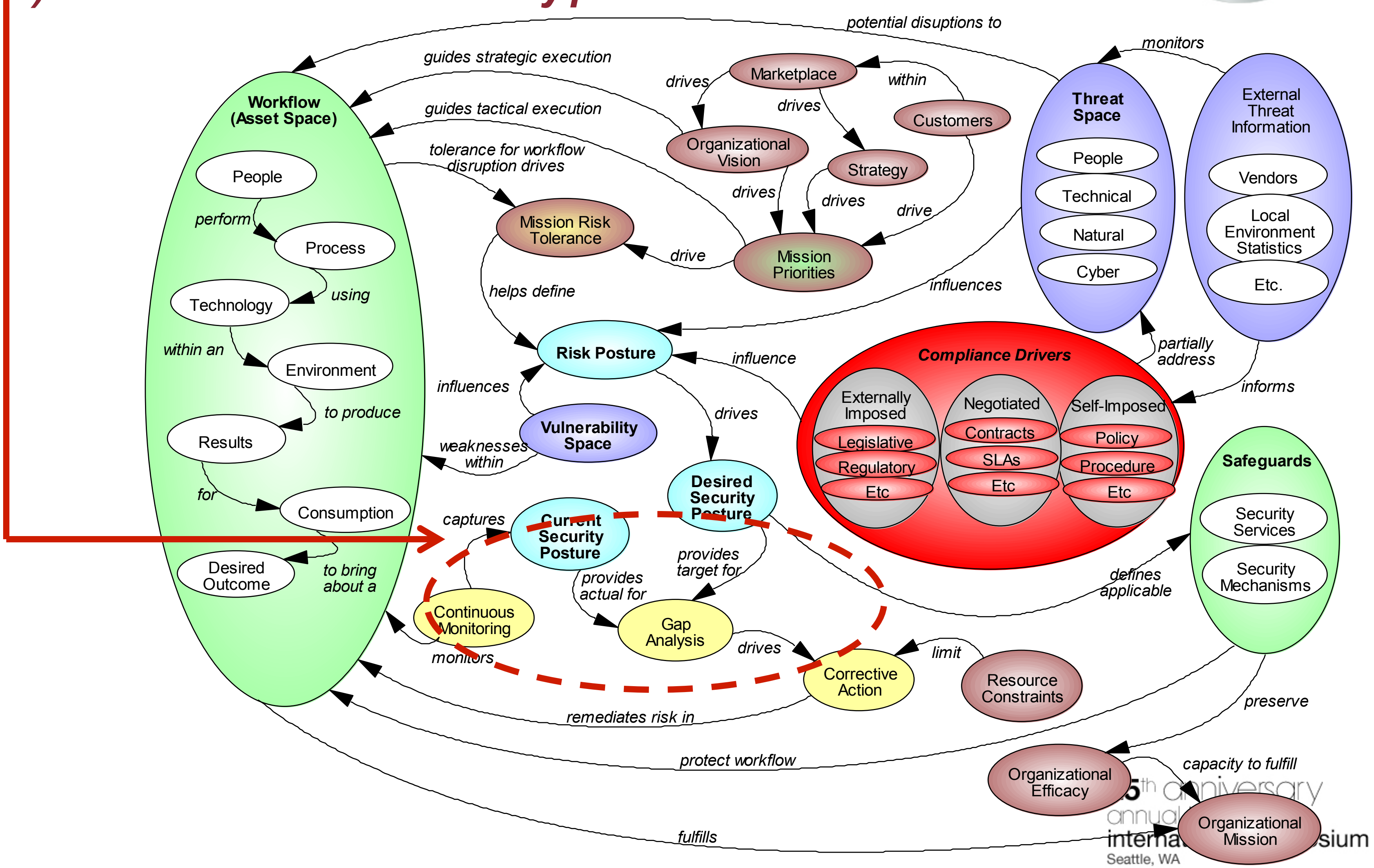
Know Yourself

Know your enemy and <u>know yourself</u> and you need not fear in a hundred battles.
– Sun Tzu


Governance
Management
Operations
Users
Practitioners
O P
O r
D o
A c
+ e
C s
2 s
Observe
Orient
Decide
Act
informs
guides
Command
Control
Data
Information
Knowledge
Understanding
Wisdom
OODA+C2
Support
Joint Cognitive System (JCS)
People-Enhanced Cognition
Machine-Enhanced Cognition
CDPs
CDPL
National Intelligence Priorities Framework (NIPF)
Priority scheme for external monitoring
Priority scheme for internal monitoring
domestic intelligence priorities framework (future)
Know the enemy
Know yourself
Intelligence Community Operations
Adversary Assets
United States Government (USG) et al. Assets
Self-Monitoring (.gov, .mil, .ic, NSS, CIKR, DIB, et al.)
Solutions
Operational Gaps
Operational Gaps
Solutions
Intelligence Community Planning & Development
U.S. Domestic-Oriented Planning & Development
Mission Operations (Workflow)
People
Process
Technology
Environment
Results
Consumption
Desired Outcome
perform
using
within
to produce
for
to bring about
Cyberspace Network Operations (CNO)
Offensive Cyberspace Operations (OCO)
Cyberspace Network Exploitation (CNE)
Cyberspace Defense / Defensive Cyberspace Operations (DCO)
Integrated Adaptive Cyberspace Defense (IACD)
observe
orient
decide
act
command
control
Active Cyberspace Defense (ACD)
Sensing
Sense-Making
Decision-Making
Acting
ACD Mgmt
Messaging & Control

Cybersecurity Ops Domains

Systems Dynamics Modeling (SDM) Oscillation Archetype



Workflow (Asset Space)
People
perform
Process
using
Technology
within an
Environment
to produce
Results
for
Consumption
to bring about a
Desired Outcome

potential disuptions to
guides strategic execution
guides tactical execution
tolerance for workflow disruption drives
Marketplace
drives
within
drives
Customers
Organizational Vision
Strategy
drives
drives
drive
Mission Risk Tolerance
drive
Mission Priorities
helps define
influences
Risk Posture
influence
influences
Vulnerability Space
weaknesses within
drives
Desired Security Posture
captures
Current Security Posture
provides target for
provides actual for
Continuous Monitoring
monitors
Gap Analysis
drives
Corrective Action
limit
Resource Constraints
remediates risk in
protect workflow
fulfills

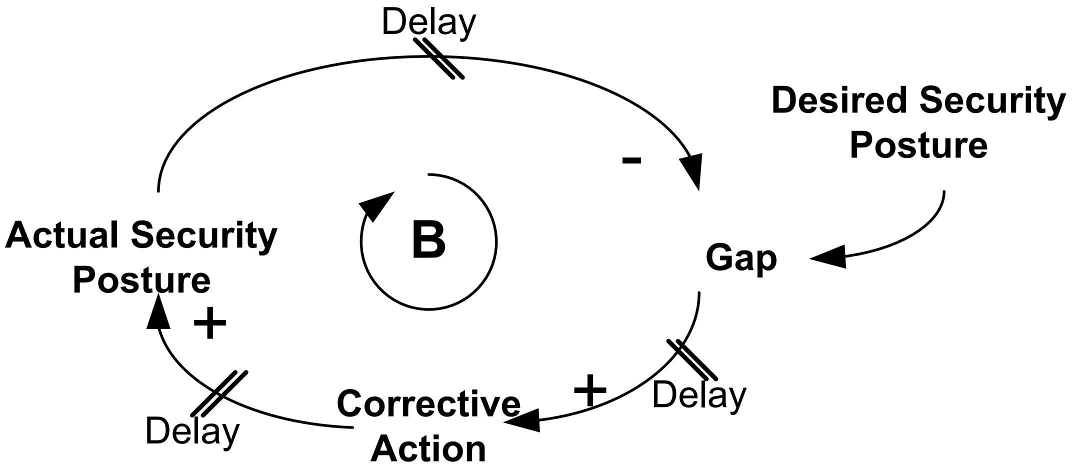
Threat Space
People
Technical
Natural
Cyber
monitors
External Threat Information
Vendors
Local Environment Statistics
Etc.
partially address
informs

Compliance Drivers
Externally Imposed
Legislative
Regulatory
Etc
Negotiated
Contracts
SLAs
Etc
Self-Imposed
Policy
Procedure
Etc

Safeguards
Security Services
Security Mechanisms
defines applicable
preserve
Organizational Efficacy
capacity to fulfill
Organizational Mission

25th anniversary annual international symposium
Seattle, WA
July 13 - 16, 2015

SDM Oscillation Archetype



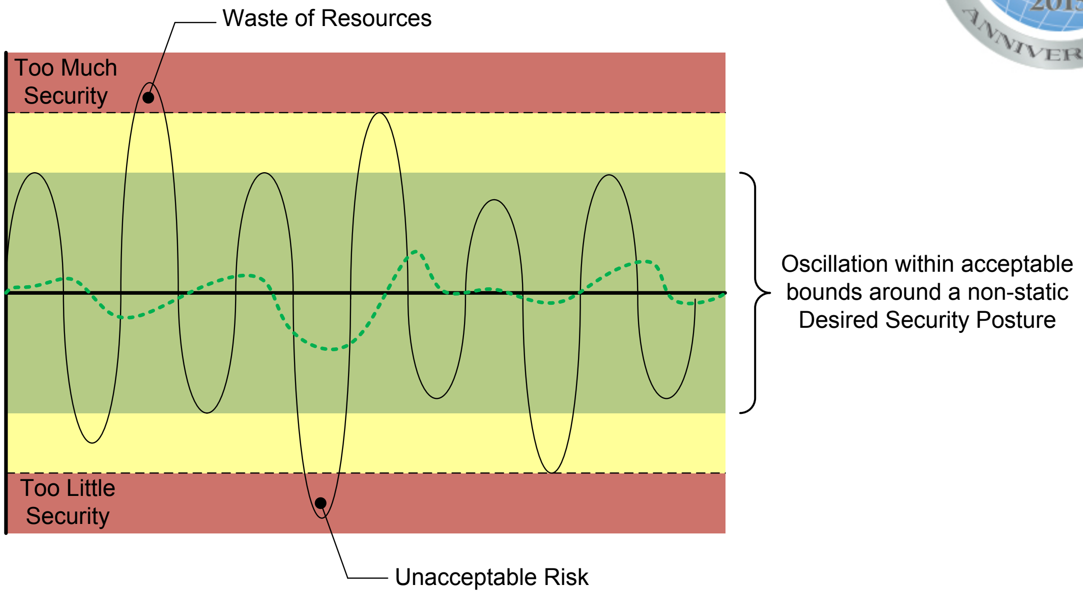
Nature of Delay

- Over-compensation
- Under-compensation

SDM Oscillation Archetype

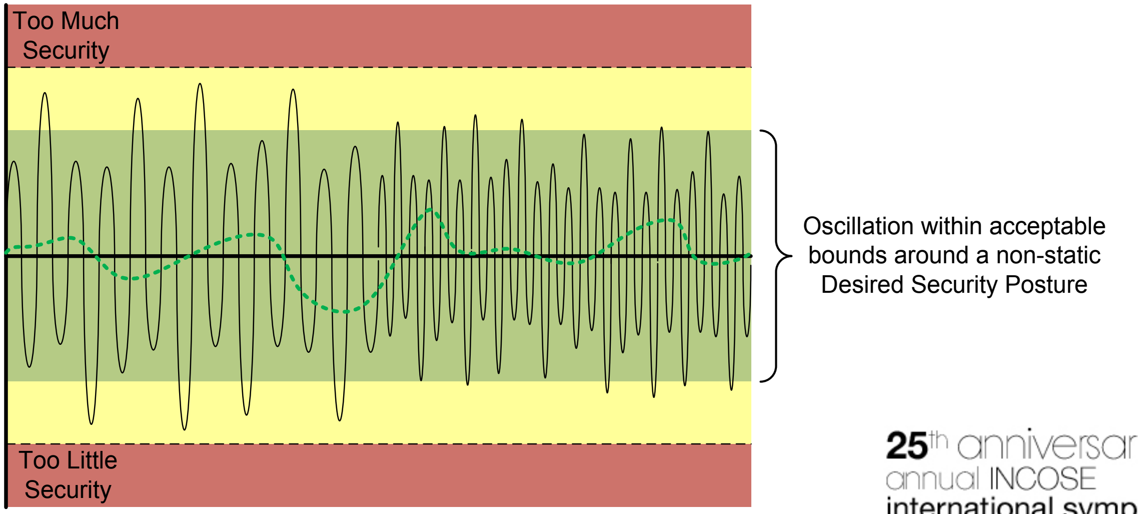
Pre-ACD/CDP

- Wide amplitude swings
- Low frequency


Waste of Resources
Too Much Security
Too Little Security
Unacceptable Risk
Oscillation within acceptable bounds around a non-static Desired Security Posture

Post-ACD/CDP

- Reduced amplitude
- Increased frequency

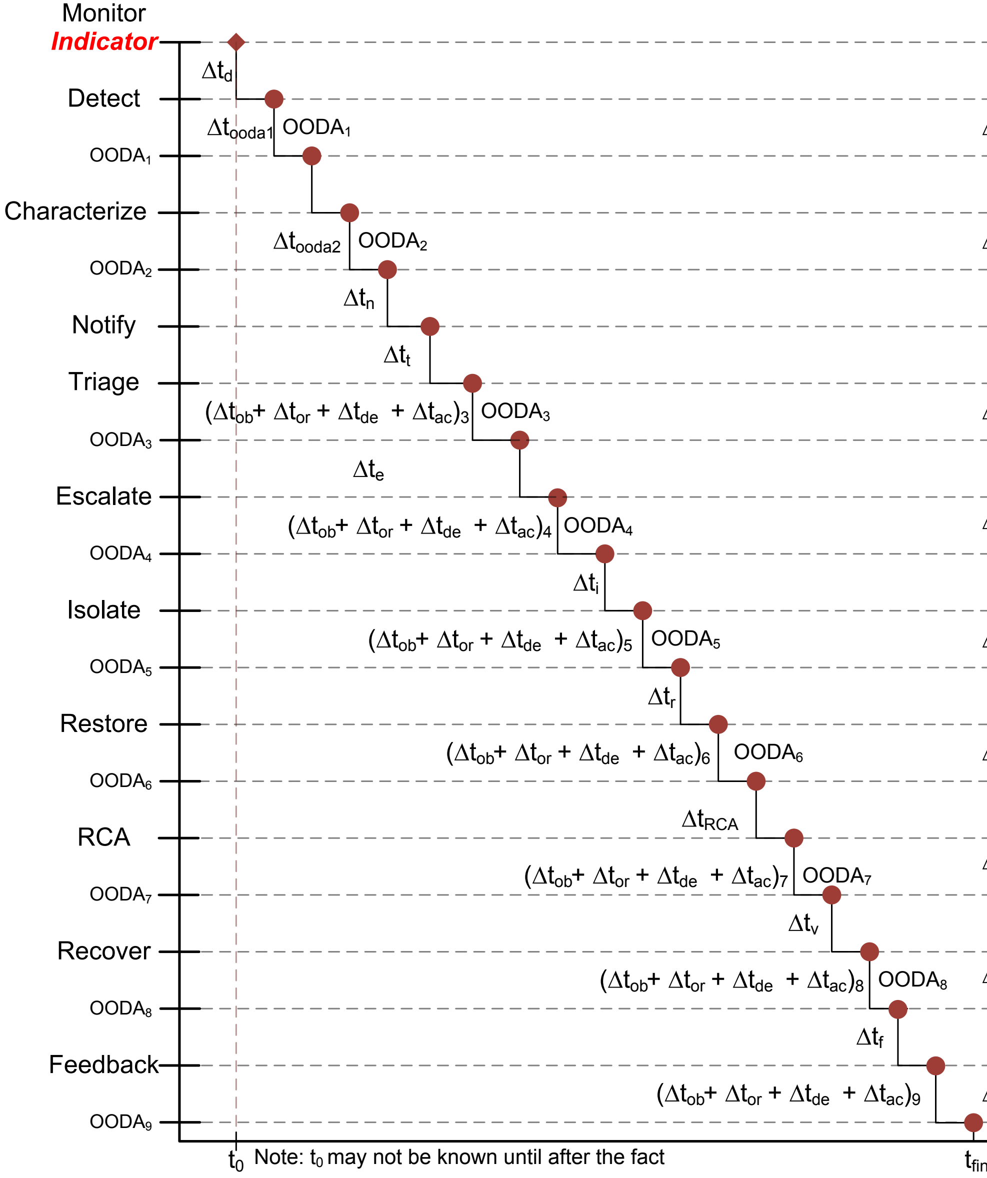

Too Much Security
Too Little Security
Oscillation within acceptable bounds around a non-static Desired Security Posture

Oscillation Archetype Instance

A View of Cybersecurity Ops Workflow

- **Monitor**: ongoing observance with intent to raise awareness
- **Detect**: indicator or anomaly
- **Characterize**: known-known, known-unknown, unknown-unknown, unknown-known
- **Notify**: first tier support
- **Triage**: determine priorities
- **Escalate**: send to subject matter expert(s)
- **Isolate**: contain threat or threat effects
- **Restore**: resume effective operations even if diminished efficiency
- **RCA**: identify root cause of problem
- **Recover**: recover effective and efficient operations to desired level
- **Feedback**: prepare organization to minimize recurrence and effects of recurrence

Time Metrics



t_0

$\Delta t_d = t_d - t_0$

$\Delta t_{ooda1} = t_{ooda1} - t_d$

$\Delta t_c = t_c - t_{de}$

$\Delta t_{ooda2} = t_{ooda2} - t_e$

$\Delta t_n = t_n - t_d$

$\Delta t_t = t_t - t_n$

$\Delta t_{ooda3} = t_{ooda3} - t_e$

$\Delta t_e = t_e - t_{ac}$

$\Delta t_{ooda4} = t_{ooda4} - t_e$

$\Delta t_i = t_i - t_{ooda4}$

$\Delta t_{ooda5} = t_{ooda5} - t_i$

$\Delta t_r = t_r - t_{ooda5}$

$\Delta t_{ooda6} = t_{ooda6} - t_r$

$\Delta t_{RCA} = t_{RCA} - t_{ooda6}$

$\Delta t_{ooda7} = t_{ooda7} - t_{RCA}$

$\Delta t_v = t_v - t_{ooda7}$

$\Delta t_{ooda8} = t_{ooda8} - t_v$

$\Delta t_f = t_f - t_{ooda8}$

$\Delta t_{ooda9} = t_{ooda9} - t_v$

t_0 is initiation of indicator
t_d is initiation of detection process
Δt_d is duration of detection process
t_{ooda2} is initiation of OODA process
Δt_{ooda2} is duration of OODA process
t_n is initiation of characterize process
Δt_n is duration of characterize process
t_{ooda2} is initiation of OODA process
Δt_{ooda2} is duration of OODA process
t_n is initiation of notify process
Δt_n is duration of notify process
t_t is initiation of triage process
Δt_t is duration of triage process
t_{ooda3} is initiation of OODA process
Δt_{ooda3} is duration of OODA process
t_e is initiation of escalate process
Δt_e is duration of escalate process
t_{ooda4} is initiation of OODA process
Δt_{ooda4} is duration of OODA process
t_i is initiation of isolate process
Δt_i is duration of isolate process
t_{ooda5} is initiation of OODA process
Δt_{ooda5} is duration of OODA process
t_r is initiation of restore process
Δt_r is duration of restore process
t_{ooda5} is initiation of OODA process
Δt_{ooda5} is duration of OODA process
t_{RCA} is initiation of root cause analysis (RCA) process
Δt_{RCA} is duration of RCA process
t_{ooda7} is initiation of OODA process
Δt_{ooda7} is duration of OODA process
t_v is initiation of recover process
Δt_v is duration of recover process
t_{ooda8} is initiation of OODA process
Δt_{ooda8} is duration of OODA process
t_f is initiation of feedback process
Δt_f is duration of feedback process
t_{ooda9} is initiation of OODA process
Δt_{ooda9} is duration of OODA process

Note: t_0 may not be known until after the fact

$t_{respond} = t_{final} - t_0$ or $t_{respond} = å\ (\Delta t_d, \Delta t_n, \Delta t_t, \Delta t_e, \Delta t_i, \Delta t_r, \Delta t_{RCA}, \Delta t_v, \Delta t_f) + å\ (\Delta t_{oooda1} \ldots \Delta t_{oooda9})$

Operational Context

Complexity & Agility

Complex

- Diverse
- Connected
- Interdependent
- Adaptive

Agile

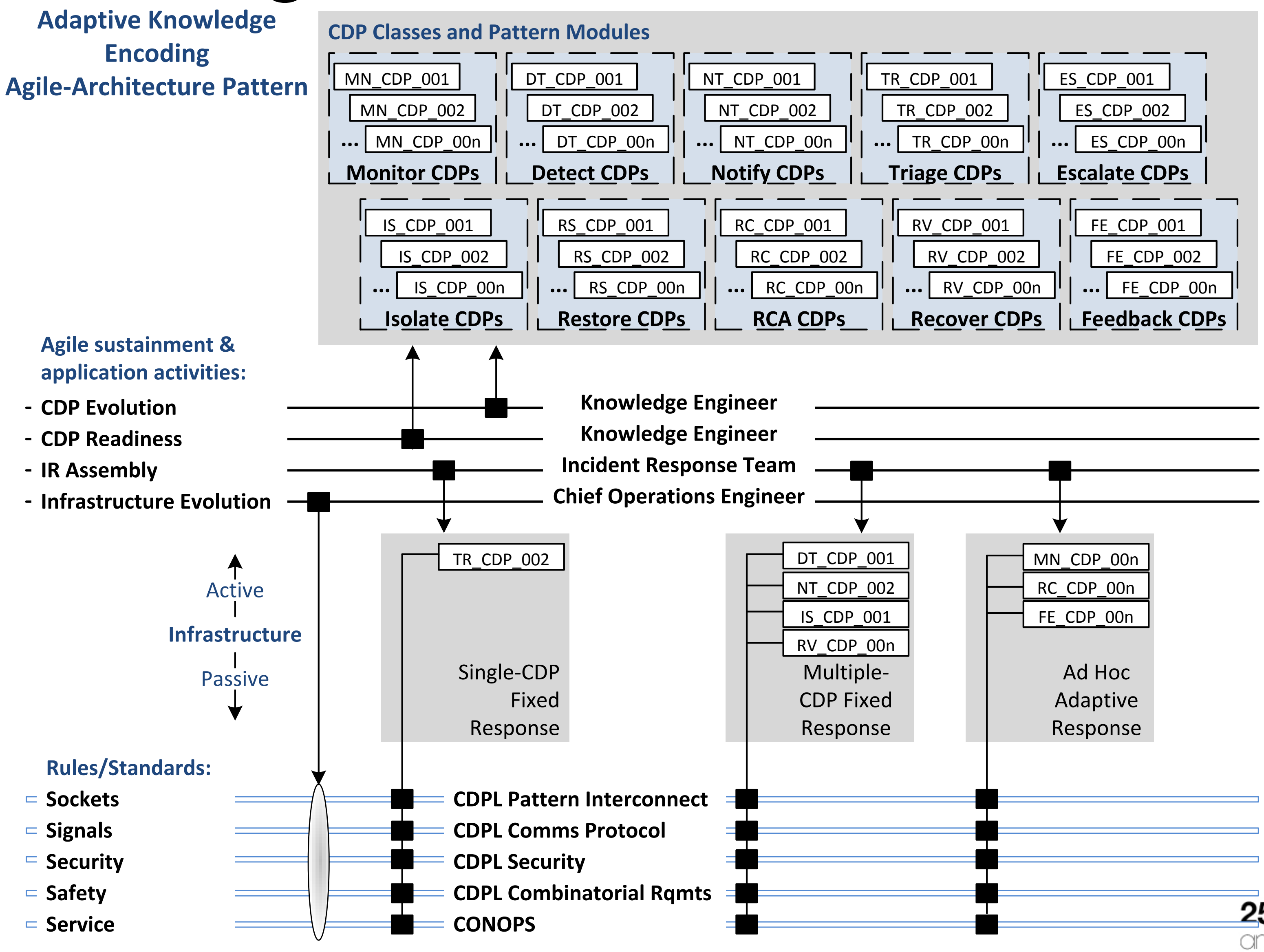
- Robust
- Resilient
- Responsive
- Flexible
- Innovative
- Adaptive

Cybersecurity operations

- Complex environment
- Constant unpredictable change

Allows organizations to thrive in an environment of constant and unpredictable change

CDP Agile-Architecture Pattern



Adaptive Knowledge Encoding
Agile-Architecture Pattern

CDP Classes and Pattern Modules

Agile sustainment & application activities:

- CDP Evolution
- CDP Readiness
- IR Assembly
- Infrastructure Evolution

Rules/Standards:

- Sockets
- Signals
- Security
- Safety
- Service

Agile Systems Engineering

- *Agile-Systems* Engineering
  - A result which is agile

- Agile *Systems-Engineering*
  - An agile development process

ACD Operational Support

- Focus: Operational Practitioners
  - E.g. operators and analysts
- Type of Support:
  - What to look for (observe)
  - How to analyze (orient)
  - How to choose (decide)
  - What to do (act)
  - How to manage (command)
  - How to direct (control)

∴OODA+C2 Support

Operational Fit to ACD

- Active Cyber Defense (ACD)
  - OODA+C2 functions
  - Joint Cognitive System (JCS)
    - Machine-Enhanced Cognition
    - People-Enhanced Cognition
      - Cybersecurity Decision Patterns (CDPs)
      - Cybersecurity Decision Pattern Language (CDPL)
- JCS facilitates continual adaptation to achieve agile cybersecurity operations

Knowledge Representation

Knowledge Repository

Data, Information, Knowledge

- Data: context-less, discrete points
- Information: context, cohesive narrative
- Knowledge: context, problem, solution
- Understanding: knowledge relationships
- Wisdom: anticipation consequences

Knowledge Management

- Part of JCS Development & Sustainment
  - Knowledge Elicitation
  - Knowledge Encoding
  - Knowledge Representation (e.g., CDPs)
  - Knowledge Repository (e.g., CDPL)
  - Knowledge Sharing
  - Knowledge Relationships (Understanding)

CDPs and the CDPL

CDP Structure

Minimal Details:

- Name
- Context
- Problem
- Solution

CDP Abbreviated Template (1 of 3)

	Description
Name	Evocative name that emerges from natural language to reference this problem/solution pairing.
Context	The situation, the circumstances in which the problem is solved. The context imposes constraints and helps identify the relative importance of the forces. The context may include tactical and strategic perspectives, for example: • Strategic ○ Organization: <organization identifier> (e.g., accounting) ○ Strategic Function: <function> (e.g., collections workflow management) ○ Capability: <details> (i.e., description of desired results) ○ Activity: <details> (i.e., formal collection of activities producing desired results; may use the generic workflow as a standard way to represent activity) ○ Task: <details> • Tactical (design note: we do not want to turn the pattern repository into a ticketing system, the details below are too detailed for a pattern. They have their place and may be referenced via some ticket # in the Examples essential element, but they belong in a complementary, separate system) ○ Physical location(s): <details> ○ Network identification: <details> ○ Tool: <details>

CDP Abbreviated Template (2 of 3)

	Description
Problem	The specific problem that needs to be solved. Describe the problem, the root need as a coarse abstraction and the specific need in less coarse terms. The problem describes the what and should not include the solution (the how). At the least, the problem description should include: • The root of the problem is… <the root of the cause… may be an archetype> to help frame the problem and to identify existing approaches to existing archetype problems • The desired result is… < express desired result agnostic of solution that produces the result> Spotting the problem: • Observables (indirect, symptoms, indicators): <details>; • Observables (direct, problem source): <details>

CDP Abbreviated Template (3 of 3)

	Description
Solution	Describe how to solve the problem; how to produce the desired result expressed in the problem. There may be multiple potential solutions; the best is relevant to the context and resolves the highest priority forces. The solution description may read like an instruction/ imperative. Notional solution structure: • Monitor: for <details> • Detect: observable <details> • Characterize: known-known, known-unknown, unknown-unknown, unknown-known • Notify: who <details> according to detect details • Triage: priority <details> according to detect details and tactical and strategic mission • Escalate: to level of expertise <details> per detect and triage details • Isolate: containment <details> according to tactical and strategic details • Restore: achieve interim operations <details> according to tactical and strategic mission • Root Cause Analysis (RCA): <details; or, explicit reference to external report> • Recover: achieve normal operations <details> • Feedback: systemic feedback <details>; CDP feedback <details>

Notional CDPL Structure (1 of 2)

IR Phase	Problem	Helps Answer Operational Questions (Knowledge Types)
Monitor	Via situational awareness, I heard to expect something…	• When should I expect it? (conditional) • How do I keep it out? (procedural) • How do I find it? (procedural)
Detect	I see something…	• What is it? (declarative) • What does it do? (declarative) • How does it do it? (declarative) • Where does it come from? (declarative, relational)
Notify	I need to raise awareness…	• Who needs to know? (declarative) • What do they need to know? (declarative) • How do I notify them? (procedural)
Triage	What are the priorities…	• How do I determine the priorities? (procedural) • What incident is most critical to address first? (relational) • How do I determine the effects to the tactical mission? (relational, procedural) • How do I determine the effects to the strategic mission? (relational, procedural)
Escalate	I need to engage the appropriate expertise…	• Have we seen this before and know what to do about it (i.e., known knowns)? (declarative) • Have we seen this before and still not characterized it (i.e., known unknown)? (declarative) • Have we not seen this before (i.e., unknown unknown)? (declarative) • Posteriori, did we see it before but failed to characterize it correctly (unknown known)? (declarative)

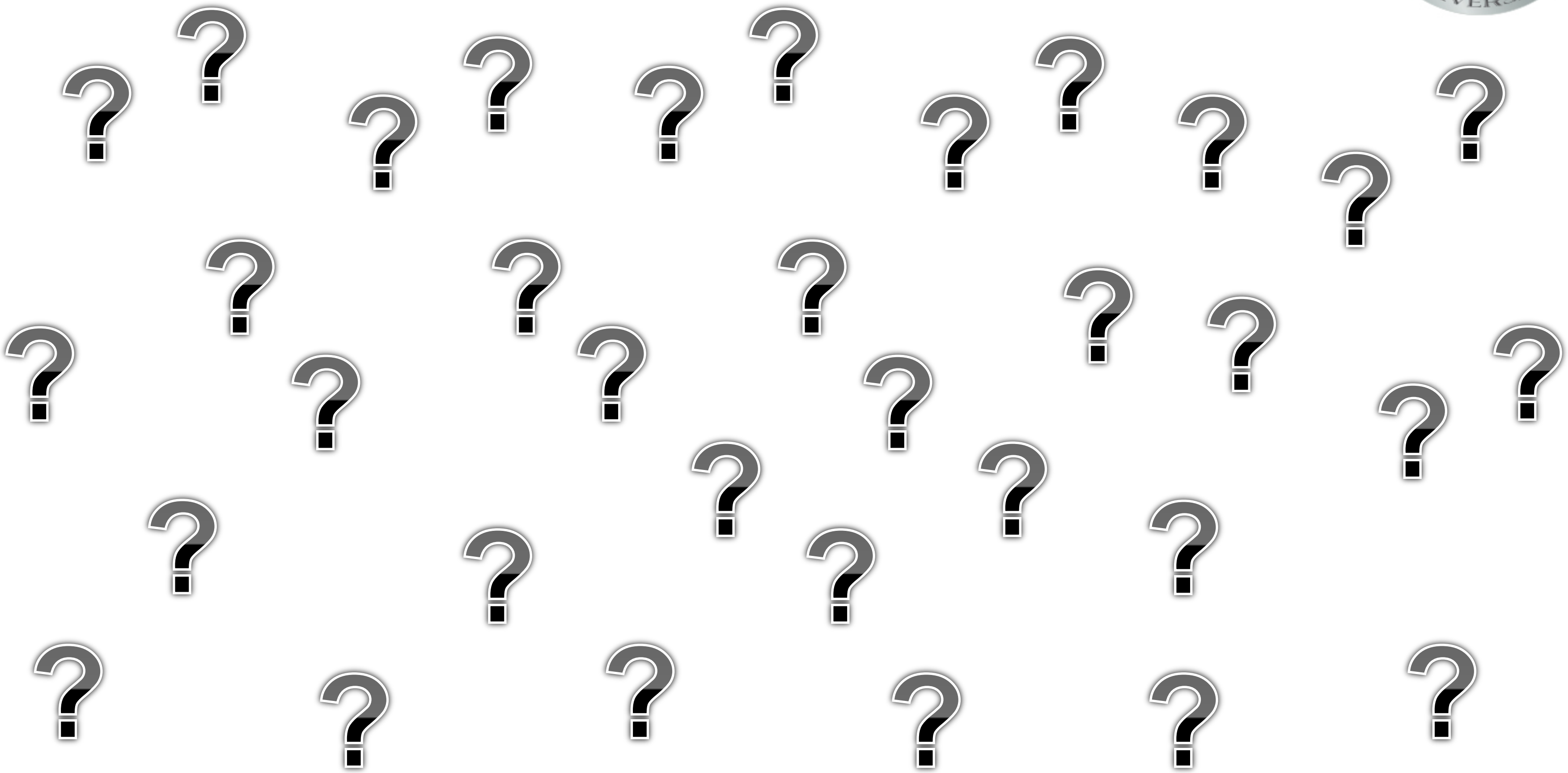
Notional CDPL Structure (1 of 2)

IR Phase	Problem	Helps Answer Operational Questions (Knowledge Types)
Isolate	I need to stop it from proliferating… I need to stop its effects from spreading…	• How do I contain it? (procedural) • How do I contain its effects? (procedural)
Restore	I need to continue operations… I need to continue to fulfill [tactical | strategic] mission…	• What is the tactical implication to mission? (declarative) • What is the strategic implication to mission? (declarative) • How do I continue the mission? How do I fight through the attack? (procedural)
Root cause analysis (RCA)	I need to find the root problem… I need to find the root cause… I need to define the root cause…	• What is the root cause? (relational) • How do I get rid of it? (procedural) • How do I reduce the probability of recurrence? (procedural) • How do I stop it from happening again? (procedural)
Recover	I need to resume normal operations…	• How do I get rid of it? (procedural) • How do I modify the operating environment to accommodate knowledge of what I found and what to do about it? (procedural)
Organizational Feedback	I need to disseminate incident details and lessons learned to others…	• How can I capture and encode incident details, the problem, and the solution? (procedural) • How do I provide details to the organization for preventive or preemptive activity to minimize recurrence? (procedural)

Summary

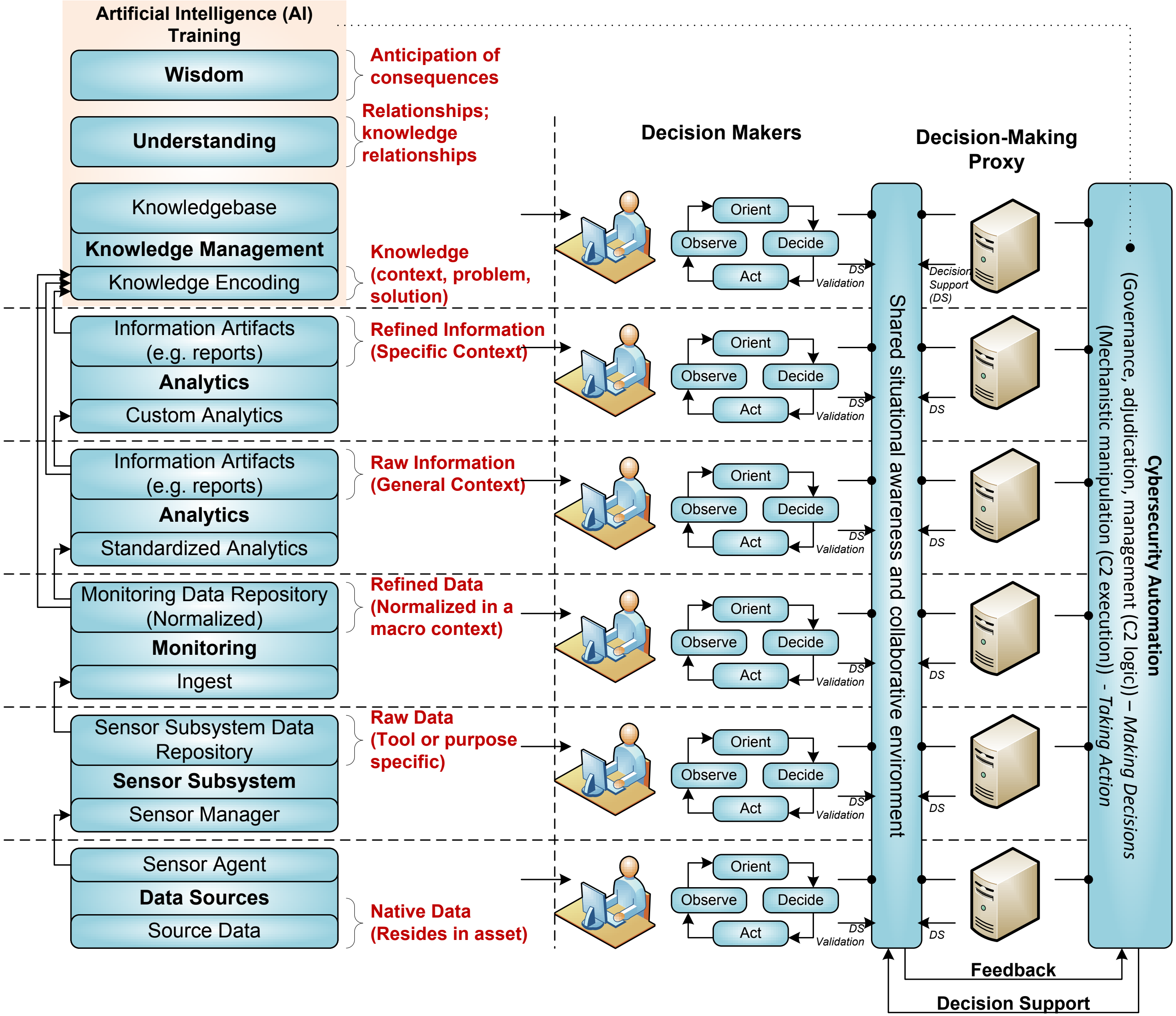
- JCS: provides OODA+C2 support
  - Part of agile cybersecurity operations
  - Machine-enhanced cognition
  - People-enhanced cognition
    - CDPs: adaptive knowledge encoding
    - CDPL: adaptive knowledge repository

Questions



Backup Slides

Knowledge



Artificial Intelligence (AI) Training

Wisdom

Anticipation of consequences

Understanding

Relationships; knowledge relationships

Knowledgebase

Knowledge Management

Knowledge Encoding

Knowledge (context, problem, solution)

Information Artifacts (e.g. reports)

Analytics

Custom Analytics

Refined Information (Specific Context)

Information Artifacts (e.g. reports)

Analytics

Standardized Analytics

Raw Information (General Context)

Monitoring Data Repository (Normalized)

Monitoring

Ingest

Refined Data (Normalized in a macro context)

Sensor Subsystem Data Repository

Sensor Subsystem

Sensor Manager

Raw Data (Tool or purpose specific)

Sensor Agent

Data Sources

Source Data

Native Data (Resides in asset)

Decision Makers

Decision-Making Proxy

Orient

Observe

Decide

Act

DS

Validation

Decision Support (DS)

Shared situational awareness and collaborative environment

Cybersecurity Automation

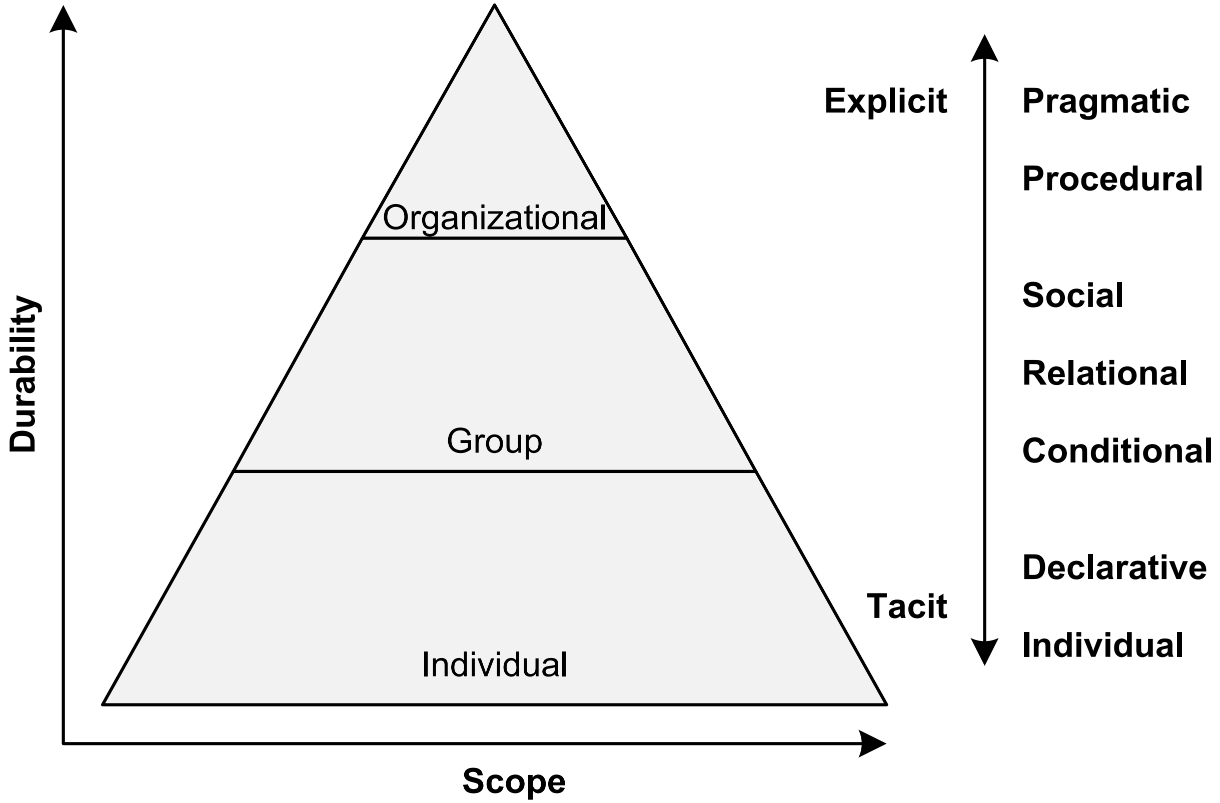
(Governance, adjudication, management (C2 logic)) – *Making Decisions*

(Mechanistic manipulation (C2 execution)) - *Taking Action*

Feedback

Decision Support

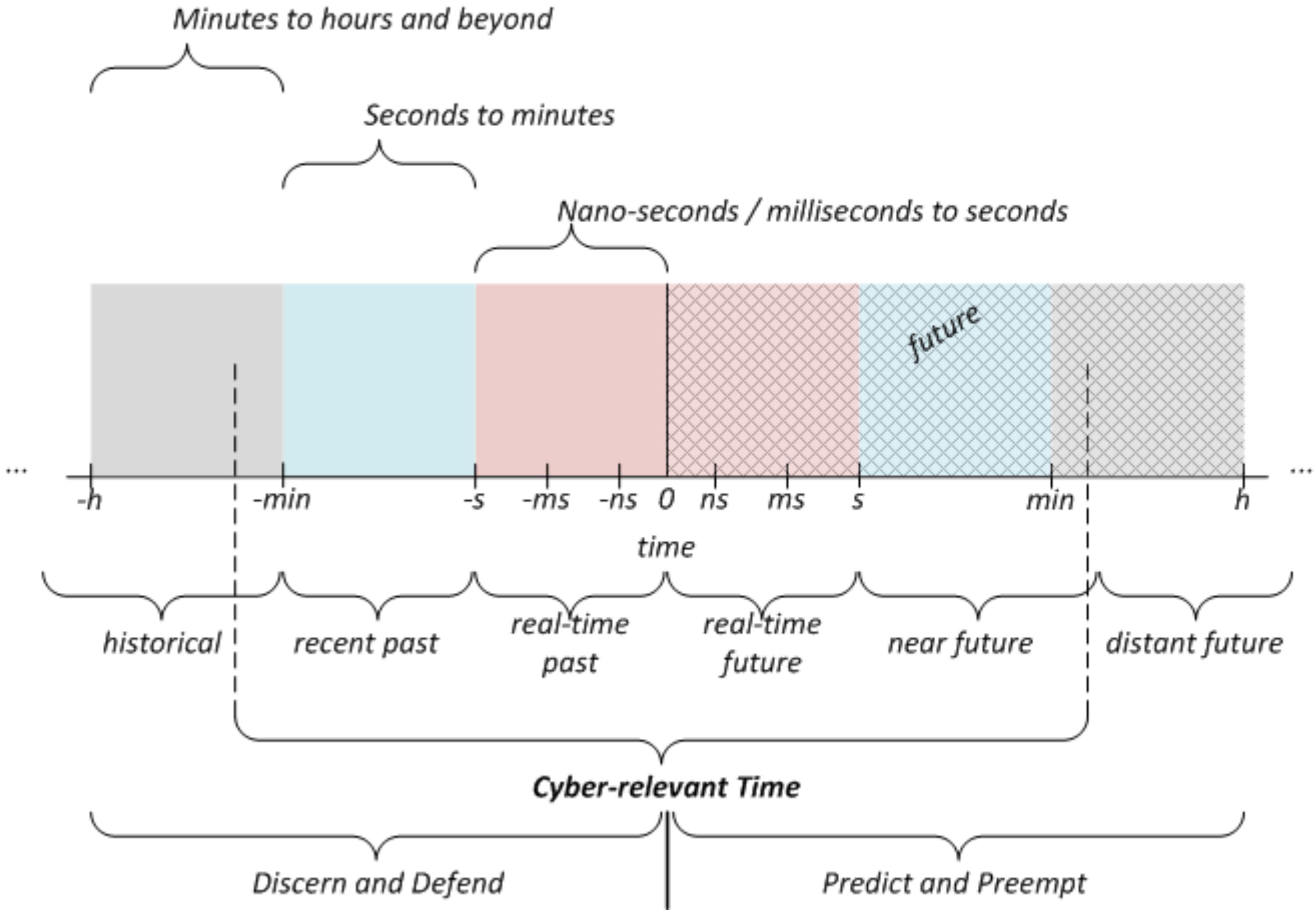
Knowledge Scales & Types



Cybersecurity Ops Knowledge

Knowledge Type	Short Description	Comments and Cybersecurity Operations Example
Pragmatic	Useful organizational knowledge	Explicit representation of best practices; e.g., codified organizational cybersecurity incident response details as derived from actual experience.
Procedural	Know-how	Explicit. Codified knowledge on security procedures; e.g., how to implement a firewall.
Social	Created by the group	Collective planning and actions; e.g., specific security mechanism acquisition, implementation, and deployment.
Relational	Know-with; interrelations	Knowledge of people, processes, and technologies interactions to achieve the desired effect; e.g., cybersecurity incident response workflow that engages multiple individuals, workgroups, and technologies. Segue from knowledge to understanding.
Conditional	Know-when	Knowledge of appropriate time to employ particular security services and mechanisms. Essence of balancing risk mitigation with resource constraints; e.g., when to add behavior-based or content-based security monitoring to signature-based.
Declarative	Know-about	Awareness of Risk Posture and associated security services and mechanisms that comprise the Security Posture (Figure 1); e.g. existence of anti-malware software or intrusion detection system.
Individual	Created by the person	More tacit. Cybersecurity operator and analyst individual practices to facilitate operations, identify malware, isolate malware, and remove it.

Cyber-Relevant Time



Future: Artificial Intelligence

- To adapt an AI system (e.g., IBM Watson) to a domain requires the following:
  1. Ingest a lexicon
  2. Ingest a corpus (body of knowledge)
  3. Ingest question/answer pairs (carefully crafted)
- Watson fundamentals: logistic regression
  - Encounters a new question…
    - …uses existing Q/A pairs to calculate a confidence level in finding same/similar questions
    - …confidence level for finding associated answers