ICCST

(46th Annual International Carnahan Conference on Security Technology)

Introduction to Self-Organizing Adaptive Systems

Plenary Session Pattern-Project Overview

Newton, MA, 15-18 Oct 2012

Rick Dove

Paradigm Shift International, and

Stevens Institute of Technology

www.parshift.com/s/121015ICCST-Patterns.pdf

A flash mob is a pick-up group of people who assemble suddenly in a designated place to perform some collective activity, generally organized via telecommunications, social media, or viral emails. The first flash mobs were created in Manhattan in 2003 as a social experiment, by Bill Wasik, senior editor of *Harper's Magazine*.

Pillow fight flash mob in Downtown Toronto (2005)

**2,000 people converged
on Dupont Circle in Washington
on 6Feb2010 for a snowball
fight of epic proportions -- responding to
messages posted on Facebook and Twitter**

www.huffingtonpost.com/2010/02/07/dupont-circle-snowball-fi_n_452638.html

www.nytimes.com/2010/03/25/us/25mobs.html

24Mar2010: Philadelphia Text-Message Flash Mob

www.nytimes.com/2010/03/25/us/25mobs.html

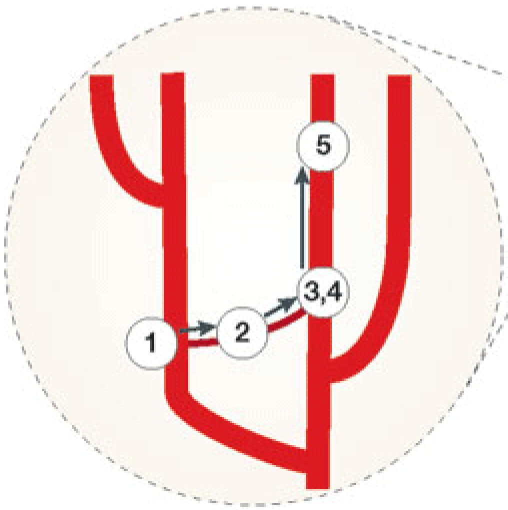
24Mar2010: Philadelphia Text-Message Flash Mob

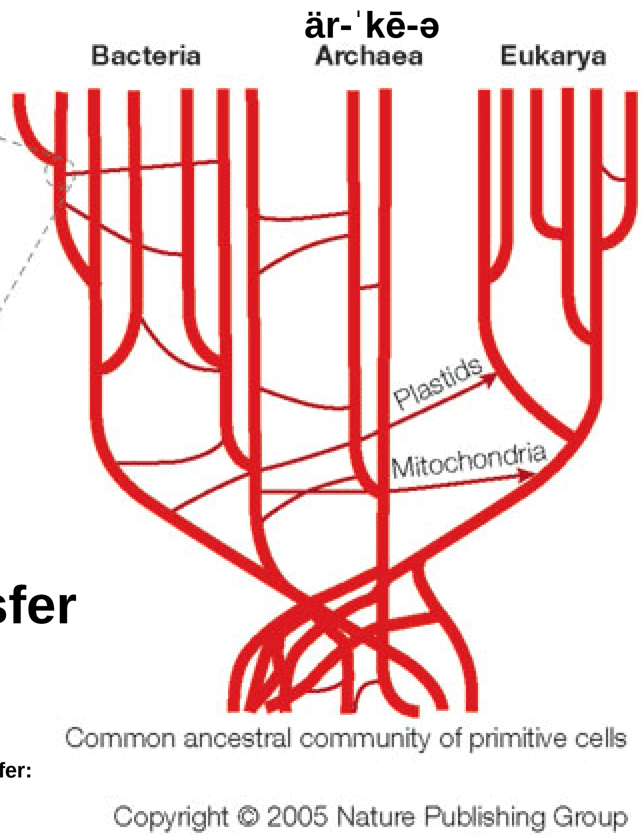
Horizontal Meme Transfer (HMT)

Evolution and Innovation

Woese, Carl. 2000. Interpreting the universal phylogenetic tree. PNAS. 97(15):8392-6. www.ncbi.nlm.nih.gov/pmc/articles/PMC26958/pdf/pq008392.pdf

Carl Woese: "Vertically generated and horizontally acquired variation could be viewed as the yin and the yang of the evolutionary process.





Horizontal Gene Transfer

"HGT"

5 steps leading to the stable inheritance of a transferred gene in a new host. Figure: Smets, Barth F. and Tamar Barkay. 2005. Horizontal gene transfer: perspectives at a crossroads of scientific disciplines. *Nature Reviews Microbiology* 3, 675-678 (Sep 2005).

"The vast majority, between 88% and 98%, of the expansions of protein families are due to HGT [in eight studied prokaryote clades]"

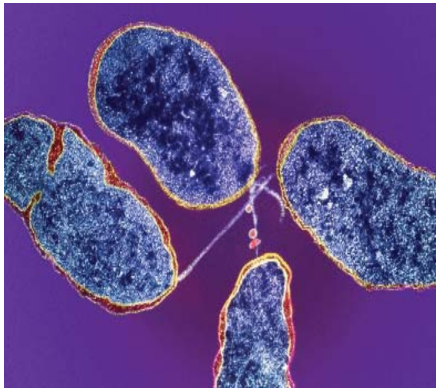
Treangen, Todd J. and Eduardo P. C. Rocha. 2011. Horizontal Transfer, Not Duplication, Drives the Expansion of Protein Families in Prokaryotes. PLoS Genetics 7:1, January.

"Vertically generated variation is necessarily highly restricted in character; it amounts to variations on a lineage's existing cellular themes.

Horizontal transfer, on the other hand, can call on the diversity of the entire biosphere, molecules and systems that have evolved under all manner of conditions, in a great variety of different cellular environments.

Thus, horizontally derived variation is the major, if not the sole, evolutionary source of true innovation."

Pattern: Horizontal Gene/Meme Transfer

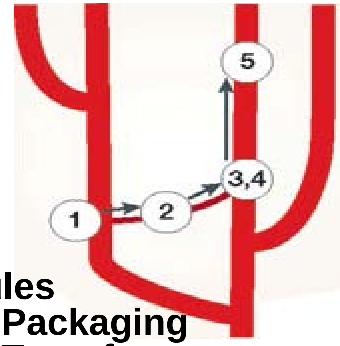


Available high variety cellular organisms

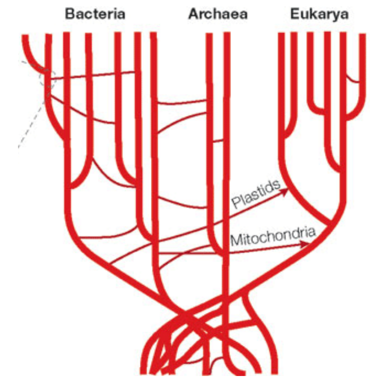
Intrachromsomal genes

Extrachromosomal genes

Two modular gene pools



Rules
1. Packaging
2. Transfer
3. Entry
4. Establishment
5. Inheritance



Innovative adaptation and evolution

Horizontal gene transfer speeds up innovative adaptation and evolution

Context: When conditions deteriorate, it makes a lot of sense to try to scavenge DNA from your neighbors. Horizontal gene transfer facilitates a fast microbial adaptation to stress. Higher-than-suspected transfer rates among microbes living in nutrient-poor environments, where sharing genes may be key to survival, has been observed. Evidence indicates that organisms limit gene exchange to microbes on nearby branches of the family tree, probably because their chromosomes share certain characteristics. Genes appear to be exchanged between species with similar chromosomal structures (Pennise 2011).

Problem: Situational or environmental changes that threaten fitness or survival.

Forces: Short-term adaptability vs. long-term-evolvability, horizontal gene transfer speeds the development of new traits by a factor of 10,000 (Woese 2000, Pennise 2011).

Solution: Incorporate appropriate material from other domains that have developed compatible and useful situational fitness. Mobile concepts don’t just help a community survive, they also provide the grist for evolutionary innovations.

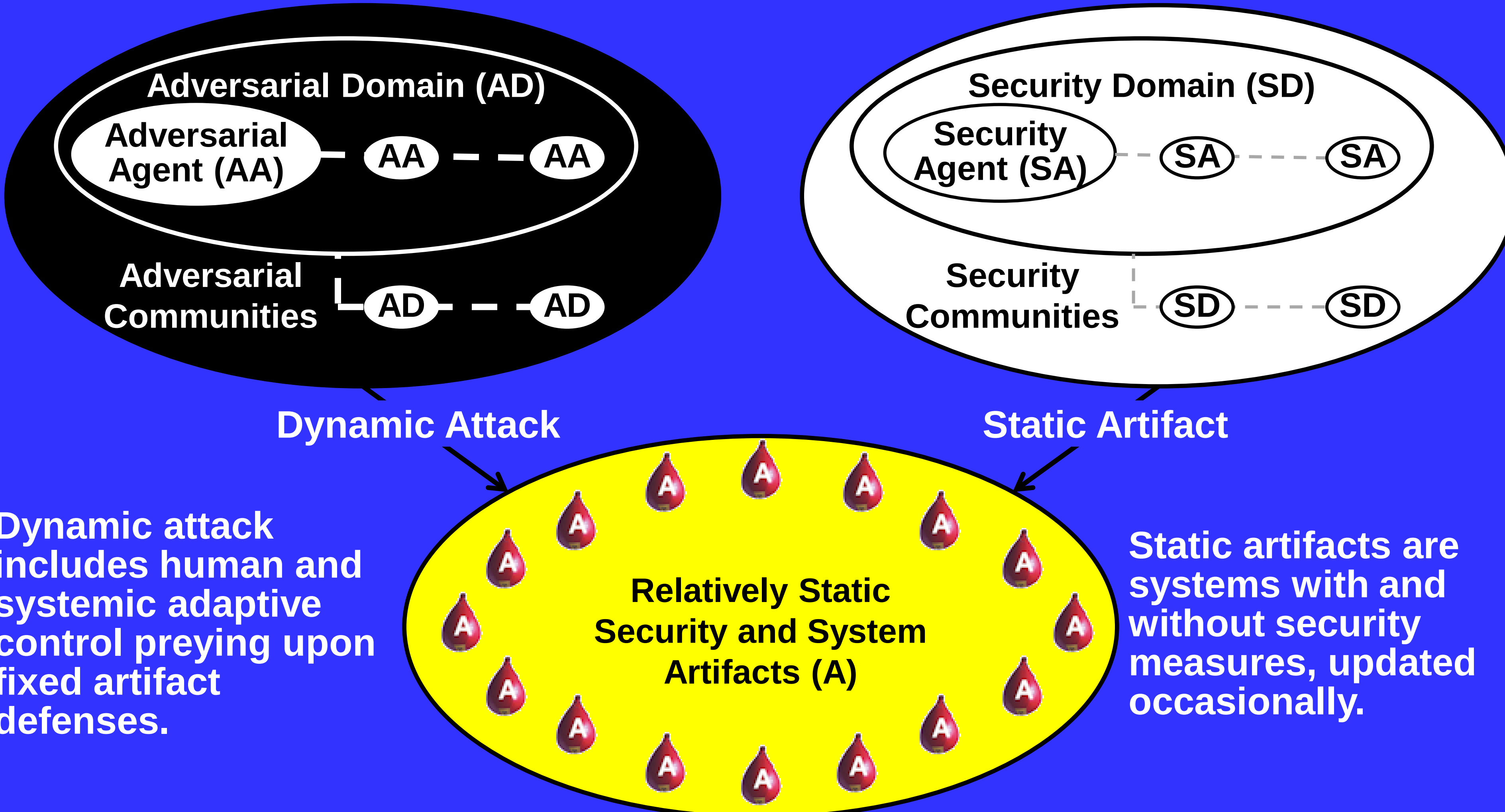
Pattern: Horizontal Gene/Meme Transfer

- Self organization is driven by natural selection of useful gene/meme transfer.
- Adaptation to immediate needs as latent genes/memes get expressed/employed.
- Reactive resilience occurs with sufficient gene/meme mix to meet needs.
- Evolution occurs in gene/meme mix with persistent expression and inheritance.
- Proactive innovation occurs with speculative acquisitions and assemblies.
- Harmony is maintained with a robust Highly-Optimized-Tolerance (Carlson & Doyle 2002) assembly repertoire.

Examples:

- **Horizontal gene transfer and evolution (Woese 2000) & (Smets 2005),** www.ncbi.nlm.nih.gov/pmc/articles/PMC26958/pdf/pq008392.pdf www.nature.com/nrmicro/journal/v3/n9/pdf/nrmicro1253.pdf
- **Cross-domain user-behavior-channeling pattern-catalog (Lockton 2009, 2010),** http://bura.brunel.ac.uk/bitstream/2438/3664/1/Lockton_SI_paper_disclaimer_added.pdf, http://danlockton.com/dwi/Download_the_cards
- **Cross-domain dynamic-system process-pattern project (Troncale 1978, 2006),** www.allbookstores.com/author/International_Conference_On_Applied_General_Systems_Research_State_Uni.html, www3.interscience.wiley.com/journal/112635373/abstract?CRETRY=1&SRETRY=0.
- **Universal patterns in human activity and insurgent events (Bohorquez 2009),** www.nature.com/nature/journal/v462/n7275/full/nature08631.html.
- **Patterns in behavioral ecology and anti-predator behavior (Blumstein 2010)** www.eeb.ucla.edu/Faculty/Blumstein/pdf%20reprints/Blumstein_2010_BE.pdf .
- **Robustness and fragility tradeoffs in evolving complex systems (Carlson & Doyle 2000),** www.pnas.org/content/99/suppl.1/2538.full.pdf+htm.

Security: General Current Situation



Dynamic attack includes human and systemic adaptive control preying upon fixed artifact defenses.

Static artifacts are systems with and without security measures, updated occasionally.

Asymmetries

Adversary is a natural system, security strategy is an artificial system.

Adversary leads with innovation and evolution.

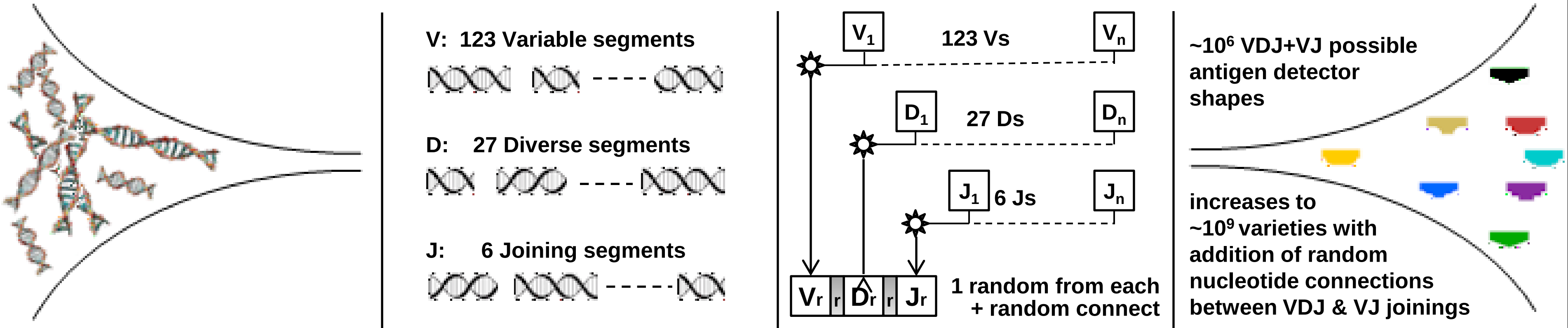
Adversary self-organizes as a dynamic system-of-systems.

Parity in Innovation and Evolution is needed.

Some Inspirational Patterns

from natural systems that effectively process noisy sensory input from uncertain and changing environments

Pattern: Bow Tie Processor (assembler/generator/mediator)



Available high variety genetic DNA input | Evolve three fixed V-D-J gene-segment libraries | Fixed-rule VDJ assembly with random interconnects | Random high variety output with VDJ + VJ assemblies

Millions of random infection detectors generated continuously by fixed rules and modules in the "knot"

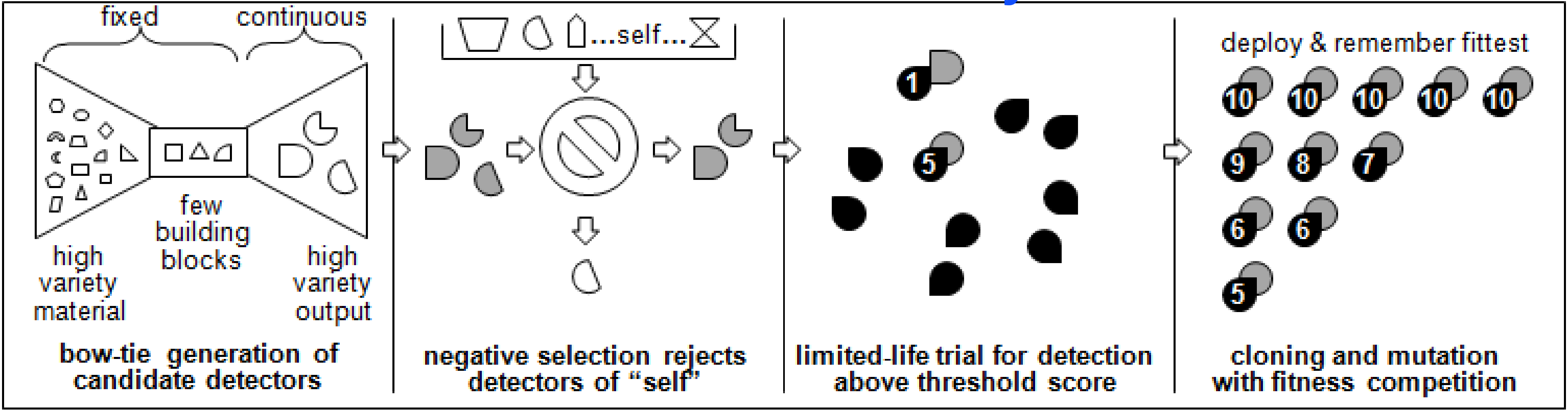
Context: Complex system with many diverse inputs and many diverse outputs, where outputs need to respond to many needs or innovate for many or unknown opportunities, and it is not practical to build unique one-to-one connections between inputs and outputs. Appropriate examples include common financial currencies that mediate between producers and consumers, the adaptable biological immune system that produces proactive infection detectors from a wealth of genetic material, and the Internet protocol stack that connects diverse message sources to diverse message sinks.

Problem: Too many connection possibilities between available inputs and useful outputs to build unique robust, evolving satisfaction-processes between each.

Forces: Large knot short-term-flexibility vs small knot short-term-controllability and long-term-evolvability (Csete 2004); robustness to known vs fragility to unknown (Carlson 2002).

Solution: Construct relatively small "knot" of fixed modules from selected inputs, that can be assembled into outputs as needed according to a fixed protocol. A proactive example is the adaptable immune system that constructs large quantities of random detectors (antigens) for unknown attacks and infections. A reactive example is a manufacturing line that constructs products for customers demanding custom capabilities.

Pattern: Proactive Anomaly Search



Speculative detector generation/mutation finds new attacks in biological immune system

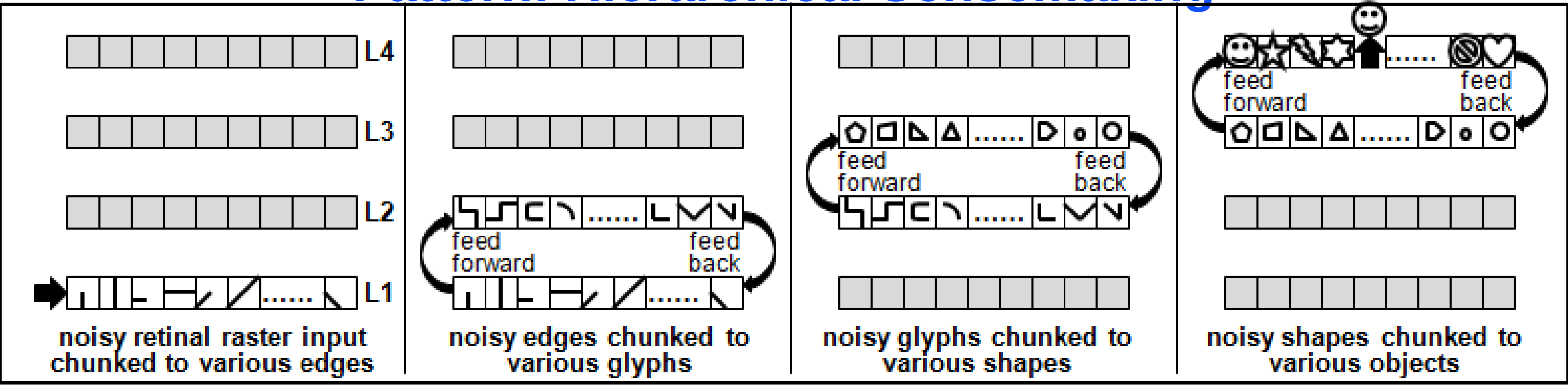
Context: A complex system or system-of-systems subject to attack and infection, with low tolerance for attack success and no tolerance for catastrophic infection success; with resilient remedial action capability when infection is detected. Appropriate examples include biological organisms, and cyber networks for military tactical operations, national critical infrastructure, and commercial economic competition.

Problem: Directed attack and infection types that constantly evolve in new innovative ways to circumvent in-place attack and infection detectors.

Forces: False positive tradeoffs with false negatives, system functionality vs functionality impairing detection measures, detectors for anything possible vs added costs of comprehensive detection, comprehensive detection of attack vs cost of false self detection.

Solution: A high fidelity model of biological immune system antibody (detection) processes that generate high quantity and variety of anticipatory speculative detectors in advance of attack and during infection, and evolve a growing memory of successful detectors specific to the nature of the system-of-interest.

Pattern: Hierarchical Sensemaking



Four level feed forward/backward sense-making hierarchy modeled on visual cortex

Context: A decision maker in need of accurate situational awareness in a critical dynamic environment. Examples include a network system administrator in monitoring mode and under attack, a military tactical commander in battle, and the NASA launch control room.

Problem: A very large amount of low-level noisy sensory data overwhelms attempts to examine and conclude what relevance may be present, most especially if time is important or if sensory data is dynamic.

Forces: amount of data to be examined vs time to reach a conclusion, number of ways data can be combined vs number of conclusions data can indicate, static sensory data vs dynamic sensory data, noise tolerated in sensory data vs cost of low noise sensory data.

Solution: Using a bow-tie process, each level looks for a specific finite set of data patterns among the infinite possibilities of its input combinations, aggregating its input data into specific chunks of information. These chunks are fed-forward to the next higher level, that treats them in turn as data further aggregated into higher forms of information chunks. Through feedback, a higher level may bias a lower level to favor certain chunks over others, predicting what is expected now or next according to an emerging pattern at the higher level. Each level is only interested in a small number of an infinite set of data-combination possibilities, but as aggregation proceeds through multiple levels, complex data abstractions and recognitions are enabled.

System Security is a Prime SO-SoS Learning Opportunity

(SO-SoS: Self Organizing System of System)

Observed Asymmetric Advantages of the Natural-System Adversary

- **Adversary leads with innovation and evolution**
- **Adversary is a natural system, current security strategy is an artificial system**
- **Adversary self-organizes as a dynamic system-of-systems**

Architecture:
Multi-agent
Loosely coupled
Self organizing
Systems-of-systems

Behavior:
Swarm intelligence
Tight learning loops
Fast evolution
Dedicated intent

Assumptions:
All systems are prey.
The goal of a "natural" SO-SoS is survival.
Fundamental natural strategies for survival are innovation and evolution.
Currently the artificial-system predator has superior "natural" strategies.
Natural systems have evolved very successful survival patterns.
Artificial-system predators have evolved very successful attack patterns.
The best Test & Evaluation is confrontation with the intelligent adversary!

Maslow's Hierarchy of Needs

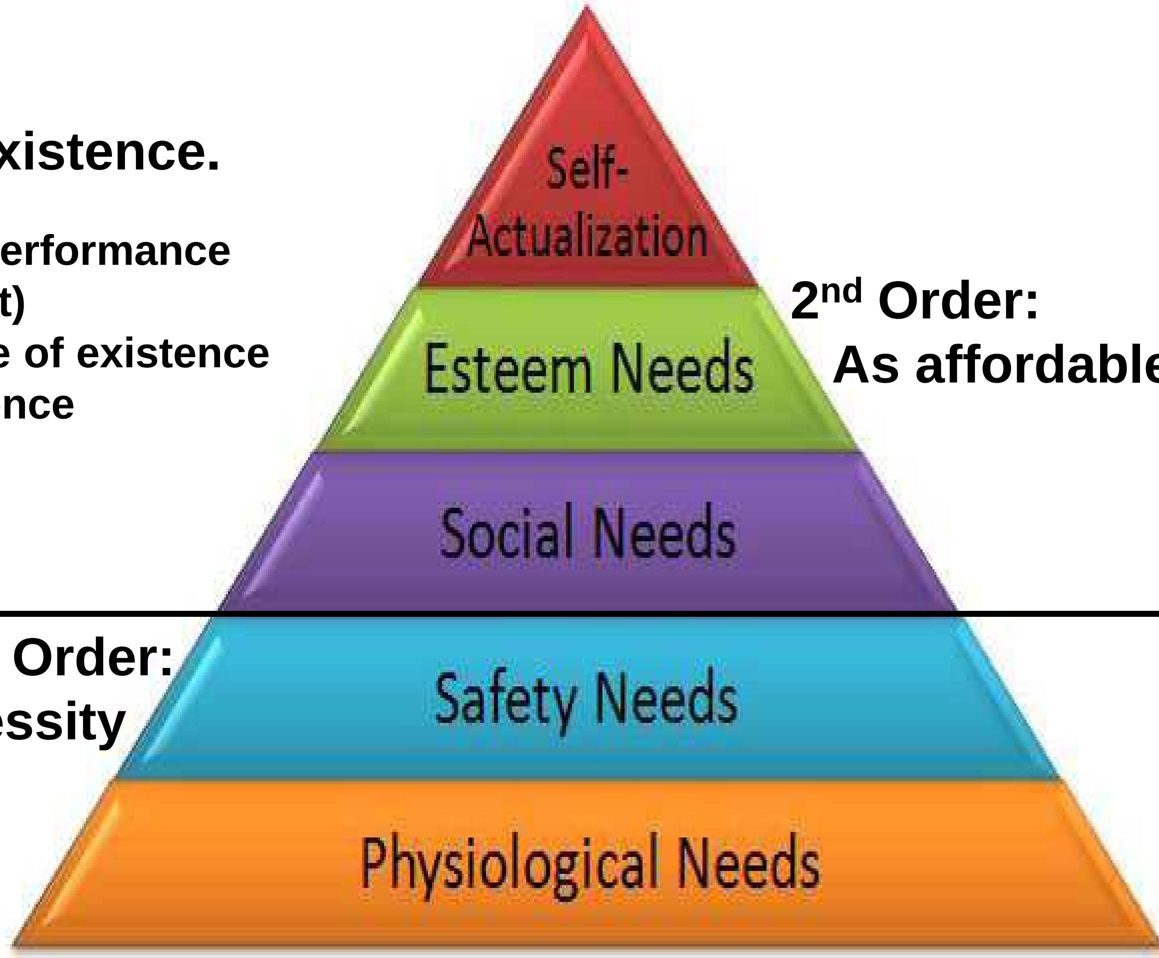
(for systems that would live one more day)

Its not about Cyber Security
…all systems are prey

Its about co-evolving
self-organizing
systems of systems,
with first priority on
securing and maintaining existence.

(5) Discretionary: non-functional performance of existence (community impact)
(4) Quality: functional performance of existence
(3) Functionality: product of existence (reason for, purpose of)
(2) Security: sustains existence
(1) Energy: enables existence

Maslow's Hierarchy of Needs



2nd Order: As affordable

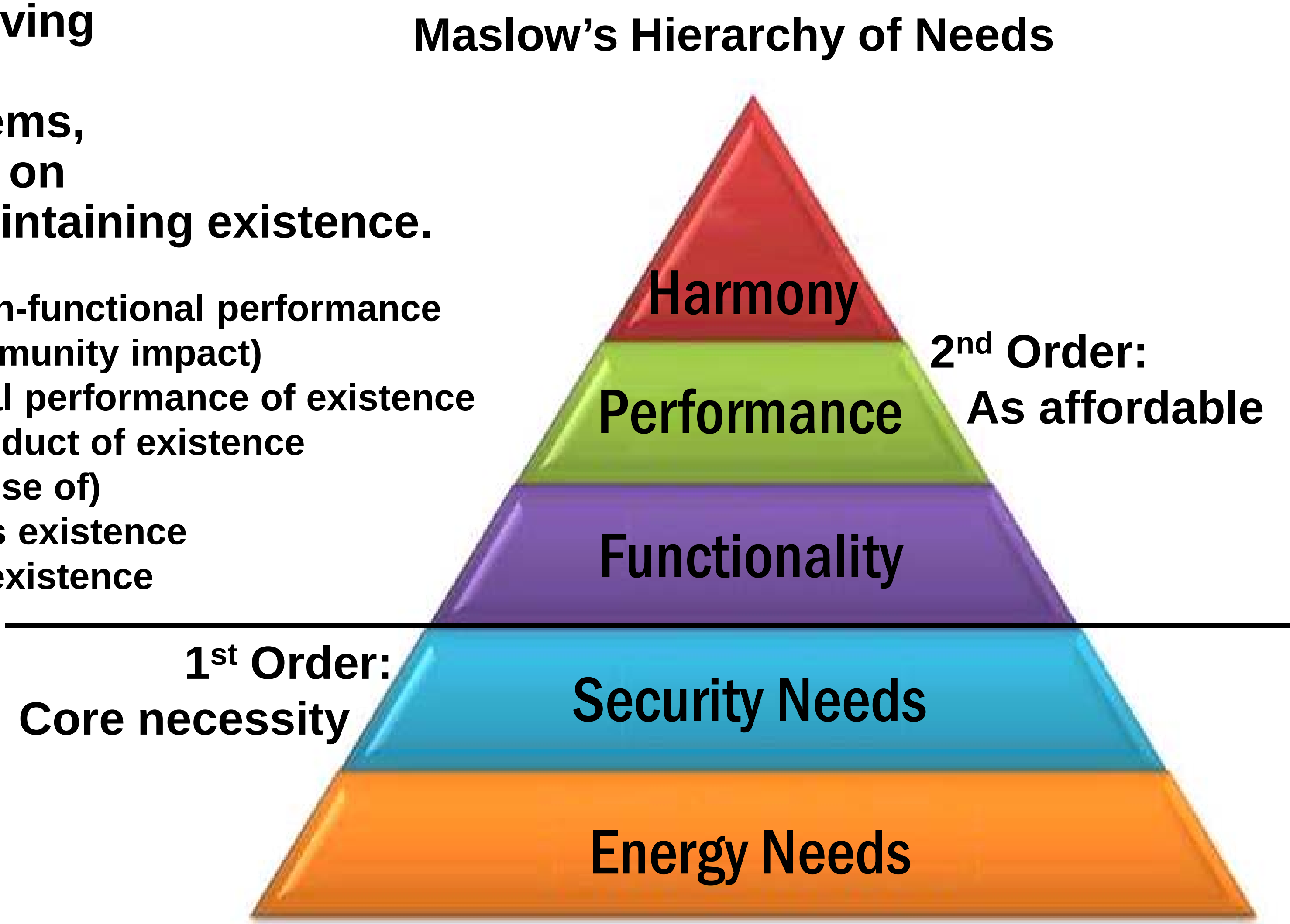
1st Order: Core necessity

Maslow's Hierarchy of Needs
(for systems that would live one more day)

Its not about Cyber Security
…all systems are prey

Its about co-evolving self-organizing systems of systems, with first priority on securing and maintaining existence.

(5) Discretionary: non-functional performance of existence (community impact)
(4) Quality: functional performance of existence
(3) Functionality: product of existence (reason for, purpose of)
(2) Security: sustains existence
(1) Energy: enables existence



Next Gen Security: Self-Organizing System of Systems

SO-SoS scares people
- but SO-SoS are all around us
- and the adversary thrives on it

SysEs, SecEs and Decision Makers don't communicate

Only SysEs can enable next gen SecE: SO-SoS

We need a common language and vision = OBJECTIVE
- for SysEs, SecEs, and Decision Makers

Patterns reflected from common understandings
- solve communication problem
- solve scary problem
- brings shared vision into focus

The Pattern Project:

- currently exploratory and candidate-discovery activity
- conducted principally by graduate students
- will transition to an INCOSE consistency-refinement and catalog product

How to Recognize a Pattern

Bob Blakley, Craig Heath, and members of The Open Group Security Forum,
Technical Guide* – Security Design Patterns, *The Open Group, 2004

[page 6] You might be wondering how you recognize a pattern if someone else hasn't already written it down. Jim Coplien recommends asking whether a solution to a problem has the following properties (if it has, it might be a pattern!):

- **Is it a solution to a problem in a context?**
- **Can you tell the problem solver what to do in order to solve the problem?**
- **Is it a mature, proven solution? In this context, ''proven'' means it has been used multiple times by architects and designers who are familiar with proper use of design patterns and on all occasions has not been found to be flawed in any way.**
- **Is it something you did not invent yourself?**
- **Does the solution build on the insight of the problem solver, and can it be implemented many times without ever being the same twice?**
- **Can the solution be formalized or automated? If it can be formalized or automated, then do that instead of writing it as a pattern.**
- **Does it have a dense set of interacting forces that are independent of the forces in other patterns?**
- **Is writing it down hard work? If it is easy to write, it may not be a pattern, or it is likely that you have not thought hard enough about the forces that bear down on the situation.**

To Start: Mirror the Enemy

Agile system security, as a minimum, must mirror the agile characteristics exhibited by the system attack community:

[S] Self-organizing – with humans embedded in the loop, or with systemic mechanisms.

[A] Adapting to unpredictable situations – with reconfigurable, readily employed resources.

[R] Reactively resilient – able to continue, perhaps with reduced functionality, while recovering.

[E] Evolving in concert with a changing environment – driven by vigilant awareness and fitness evaluation.

[P] Proactively innovative – acting preemptively, perhaps unpredictably, to gain advantage.

[H] Harmonious with system purpose – aiding rather than degrading system and user productivity.

www.parshift.com/Files/PsiDocs/Pap100226-AgileSecuritySelfOrganizingCoEvolution-ExtAbst.pdf

Name:	Descriptive name for the pattern.
Context:	Situation that the pattern applies to.
Problem:	Description of the problem.
Forces:	Tradeoffs, value contradictions, constraints, key dynamics of tension & balance.
Solution:	Description of the solution.
Graphic:	A depiction of response dynamics.
Examples:	Referenced cases where the pattern is employed.
Agility:	Evidence of SAREPH characteristics that qualify the pattern as agile.
References:	Literature access to examples.

www.parshift.com/Files/PsiDocs/Pap100317Cser-OnDiscoveryAndDisplayOfAgileSecurityPatterns.pdf

Grounding the Pattern Investigation
with a
Hierarchical Sense-Making IDS Application

SornS
(self-organizing resilient network sensing)

a maturing platform for many
work-in-process self-organizing security patterns

Chosen Because

New associative memory pattern processor opens new opportunities:

- **parallel: any number of simultaneous patterns-in-process**
- **capacity: one chip = millions of multi-feature patterns**
- **complexity: FSM patterns of any length and structure**
- **scalable: unbounded multiple chips**
- **speed: data stream rates (but not optical…yet)**
- **switching: instant save and restore for interleaved flow work-in-process**
- **Wattage: low**
- **cost: low**

Timely irresistible challenge:

Human expertise is pattern based, not reasoning based

Expertise appears to require 200,000 to 1 million patterns

Recognition needs to be instant

Learning can take some time

Knowledge must improve in time

Cortical pattern recognition appears to be hierarchical temporal memory

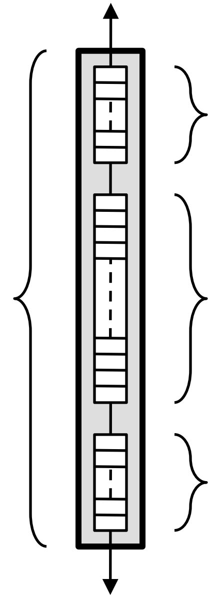
Patterns appear to consist of sparse (minimal overlap) anomalies (relatively rare occurrences)

Reconfigurable Associative-Memory Pattern Processor

Reusable Cells Reconfigurable in a Scalable Architecture

Independent **multi-feature detector** (**MFD**)
content addressable
by current input byte

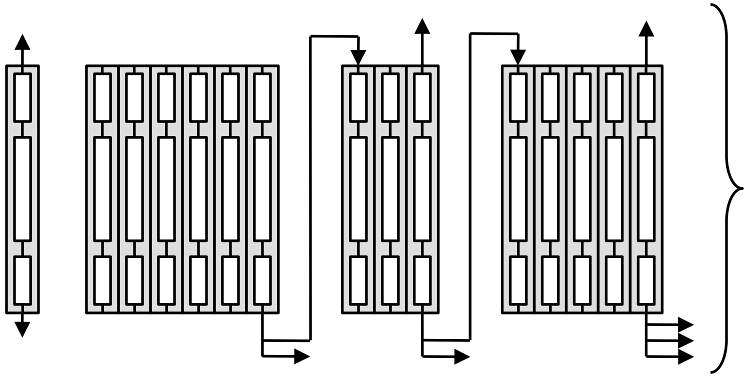
If active, and satisfied with current byte,
can activate
other designated MFDs
including itself



Pattern-satisfaction
output pointers

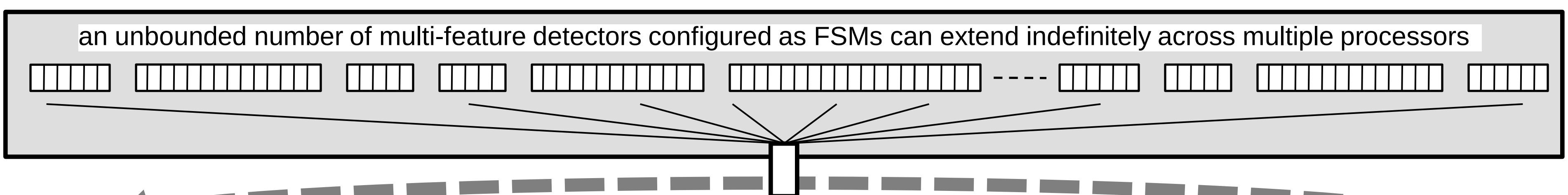
Up to 256 possible features
can be "satisfied" by any/all
"**feature indicators**" that are set

Feature-satisfaction
activation pointers



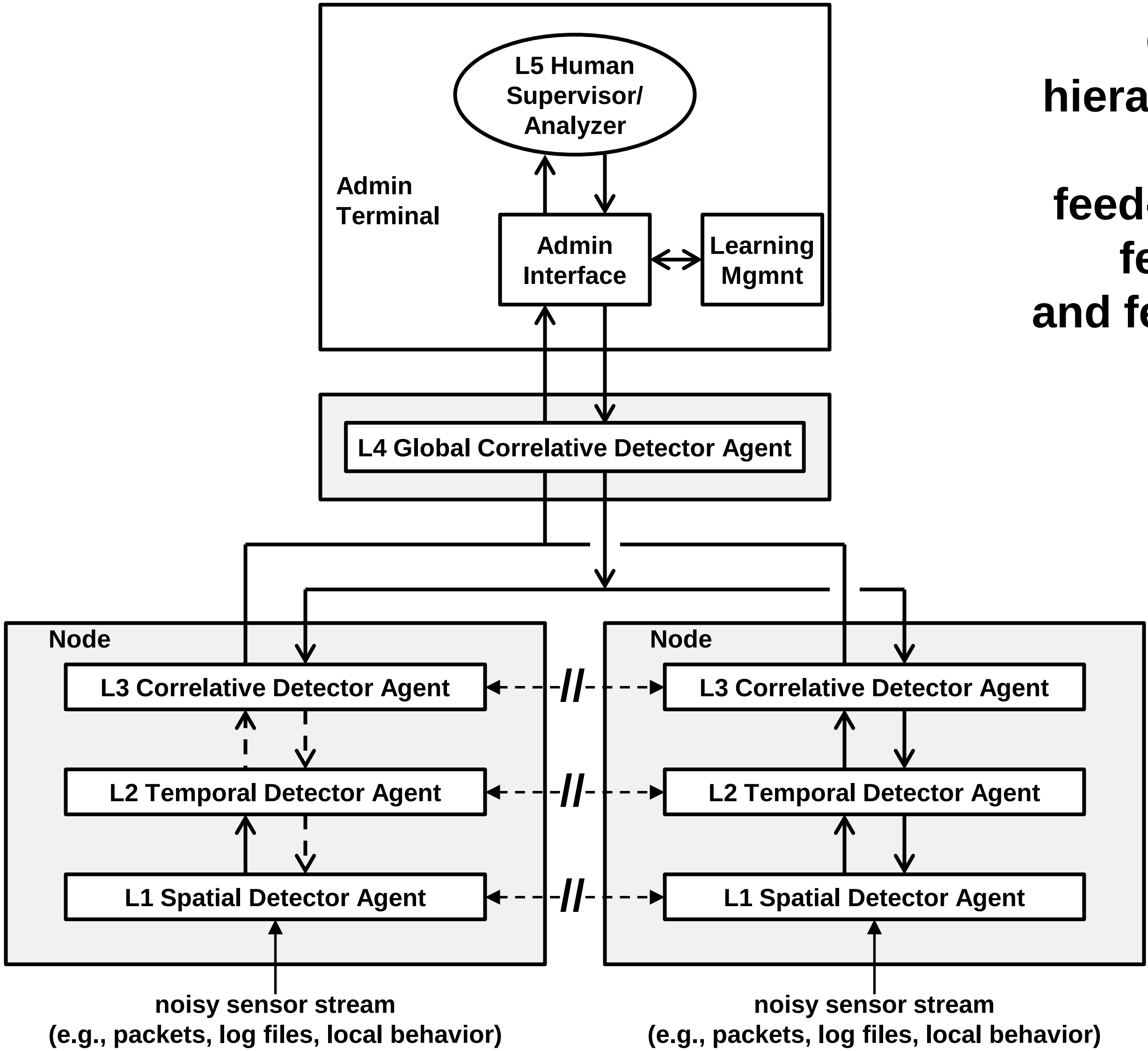
Individual MFDs
are configured into finite state machines *(FSMs)*
by linking activation pointers

- Unbounded pattern capacity
- Detection at full data stream speed
- Simultaneous detection of all active patterns



All <u>active</u> MFDs have simultaneous access to current data-stream byte

Grounded Application Target
Self Organizing Resilient Network Sensing (SornS)



General purpose hierarchical sense-making with feed-forward recognition, feed-back learning, and feed-side collaboration

Correlative: n events in any order.

Temporal: n events in order.

Spatial: n events in contiguous order.

Patterns Influencing SornS Development

1. **Dynamic Phalanx Shield**
   www.parshift.com/Files/PsiDocs/Pap100317Cser-OnDiscoveryAndDisplayOfAgileSecurityPatterns.pdf
2. **Peer-Peer Behavior Monitoring**
   www.parshift.com/Files/PsiDocs/Pap100317Cser-OnDiscoveryAndDisplayOfAgileSecurityPatterns.pdf
3. **Swarming Threat Sensors**
   ww.parshift.com/Files/PsiDocs/Pap100317Cser-OnDiscoveryAndDisplayOfAgileSecurityPatterns.pdf
4. **Drag-and-Drop Modules and Framework**
   www.parshift.com/Files/PsiDocs/PatternQualificationsForAgileSecurity.pdf
5. **Hierarchical Sense Making**
   www.parshift.com/s/110411PatternsForSORNS.pdf
6. **Proactive Anomaly Search**
   www.parshift.com/s/110411PatternsForSORNS.pdf
7. **Bow Tie Processor (assembler/generator/mediator)**
   www.parshift.com/Files/PsiDocs/PatternQualificationsForAgileSecurity.pdf
8. **Crowd Sourced Incident Reporting**
   www.parshift.com/s/110620ArchitecturalPatternsForSOSoS.pdf
9. **Swarm Discovery and Cooperation**
   www.parshift.com/s/110620ArchitecturalPatternsForSOSoS.pdf
10. **Collaborative Learning**
   www.parshift.com/s/110620ArchitecturalPatternsForSOSoS.pdf
11. **Stigmergic Interaction (4 sub-types)**
   www.parshift.com/s/110620AdversarialStigmergyPatterns.pdf
12. **Horizontal Gene/Meme Transfer**
   webinar: www.parshift.com/s/TowardsSystemicWillToLive.pdf
13. **Genetic Algorithm, ICCST 2012**
   www.parshift.com/s/121015ICCST-GeneticAlgorithm.pdf
14. **Combined Genetic-Algorithm-Neural-Network, ICCST 2012**
   www.parshift.com/s/121015ICCST-GANN.pdf
15. **Quorum Sensing, ICCST 2012**
   www.parshift.com/s/121015ICCST-QuorumSensing.pdf
16. **Peer Policing, Steve DiRose and Rick Dove (to be submitted somewhere, sometime)**

Wednesday Session 8B: Advanced Technologies and Adaptive Systems

Patterns are shown as applicable to SornS (a work in process)