

Toward a Systemic Will to Live

Rick Dove

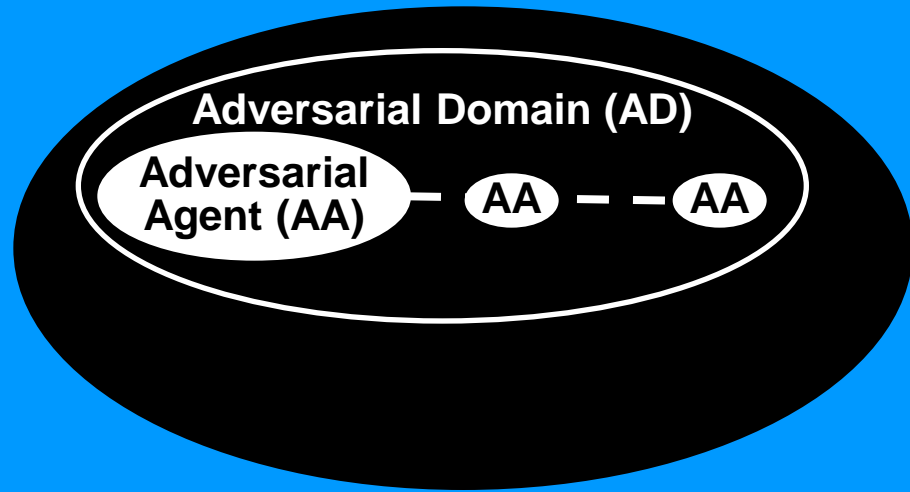
**Panel presentation at workshop on
Rethinking Cybersecurity: A Systems-Based Approach,**

**sponsored by
Center for Risk Management of Engineering Systems
and
the Institute for Information Infrastructure Protection (I3P).**

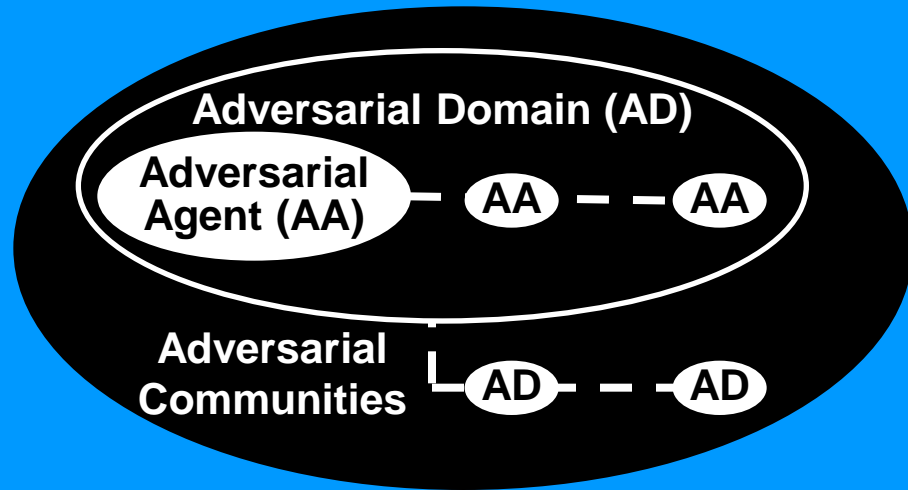
University of Virginia, Charlottesville, VA.

November 16 – 17, 2010

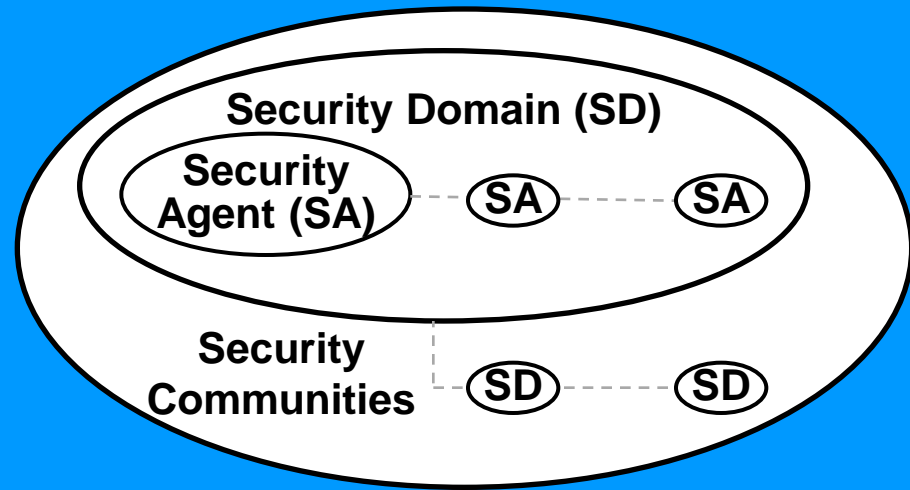
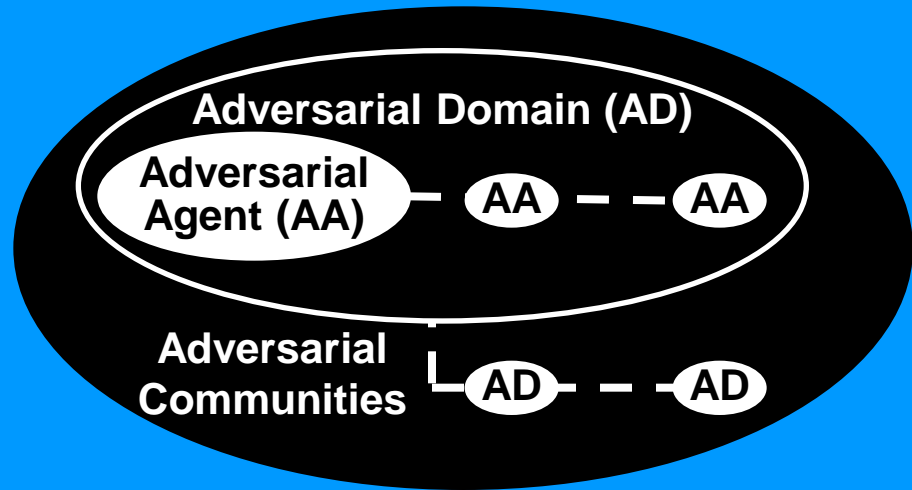
General Current Situation



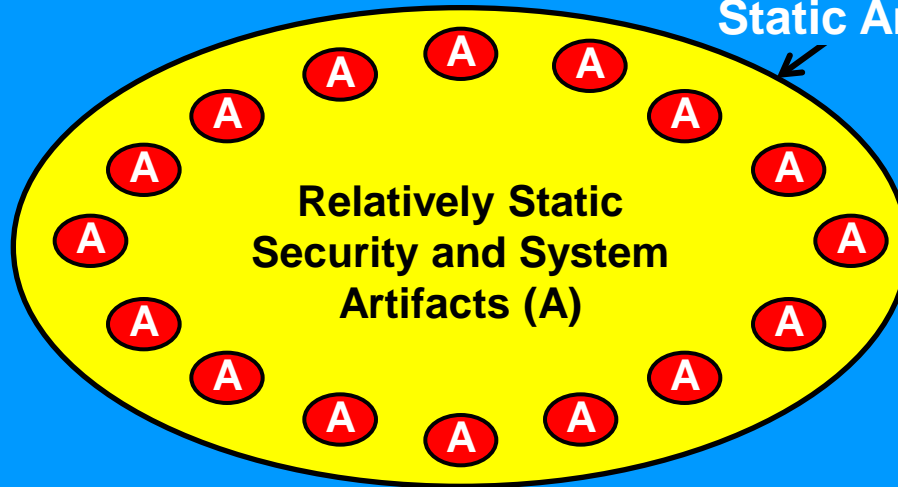
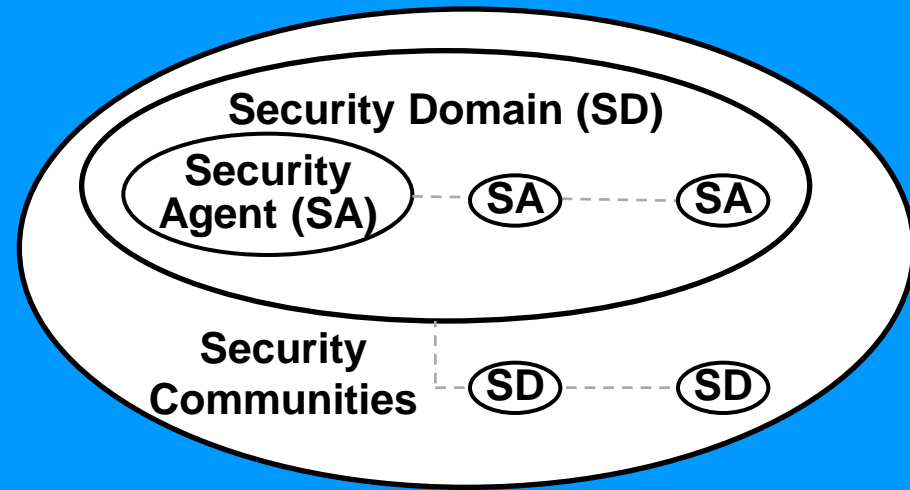
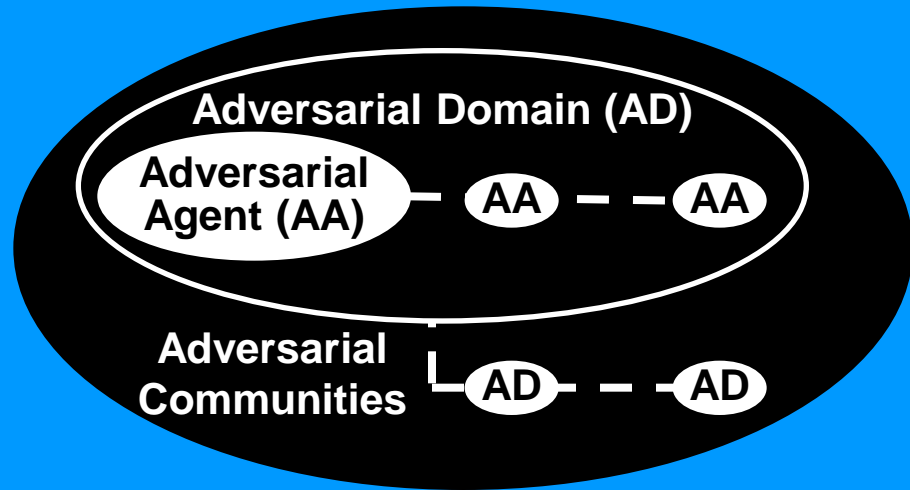
General Current Situation



General Current Situation



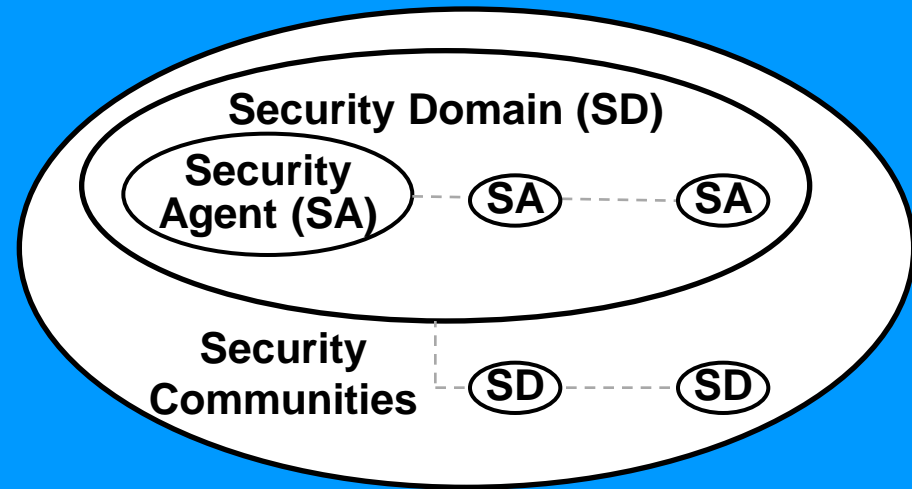
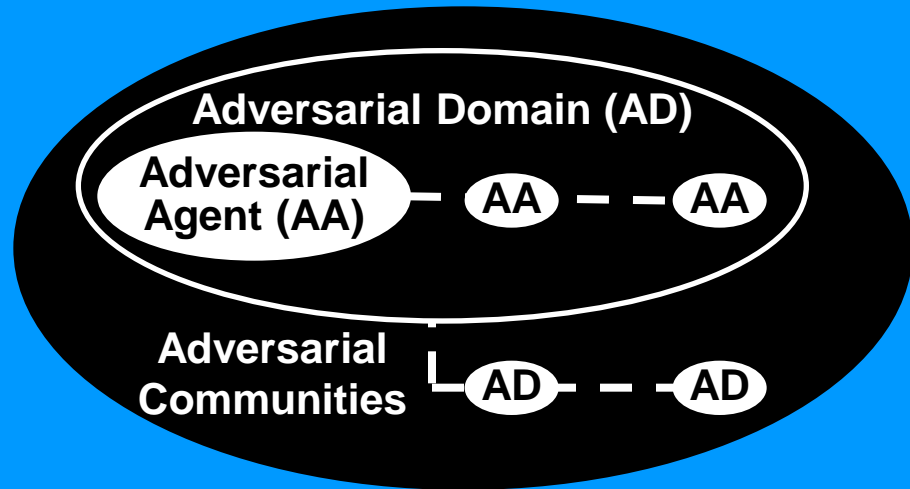
General Current Situation



Static Artifact

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

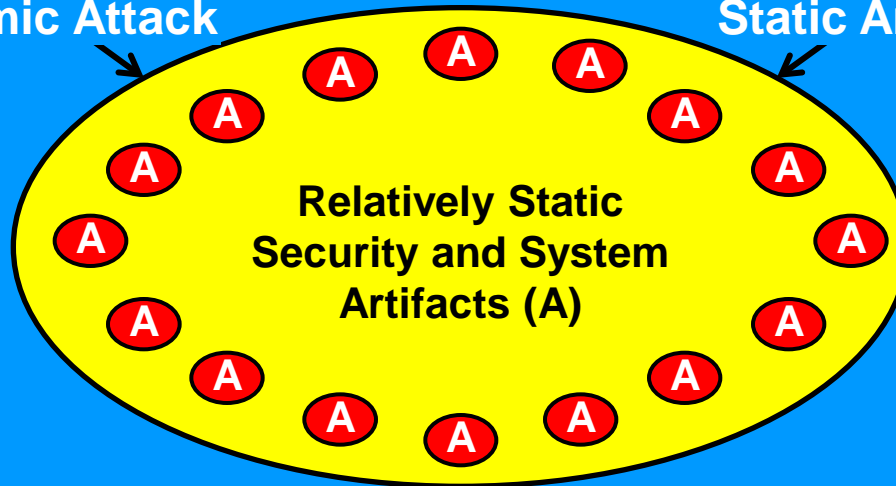
General Current Situation



Dynamic Attack

Static Artifact

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

This Talk

Project: Self organizing System-of-System Security Patterns

Project: Pattern employment proof of concept



System Engineer

Security Engineer



Decision Maker

Security Engineer



Maslow's Hierarchy of Needs



Art: www.abraham-maslow.com/m_motivation/Hierarchy_of_Needs.asp

Maslow's Hierarchy of Needs

(for systems that would live one more day)

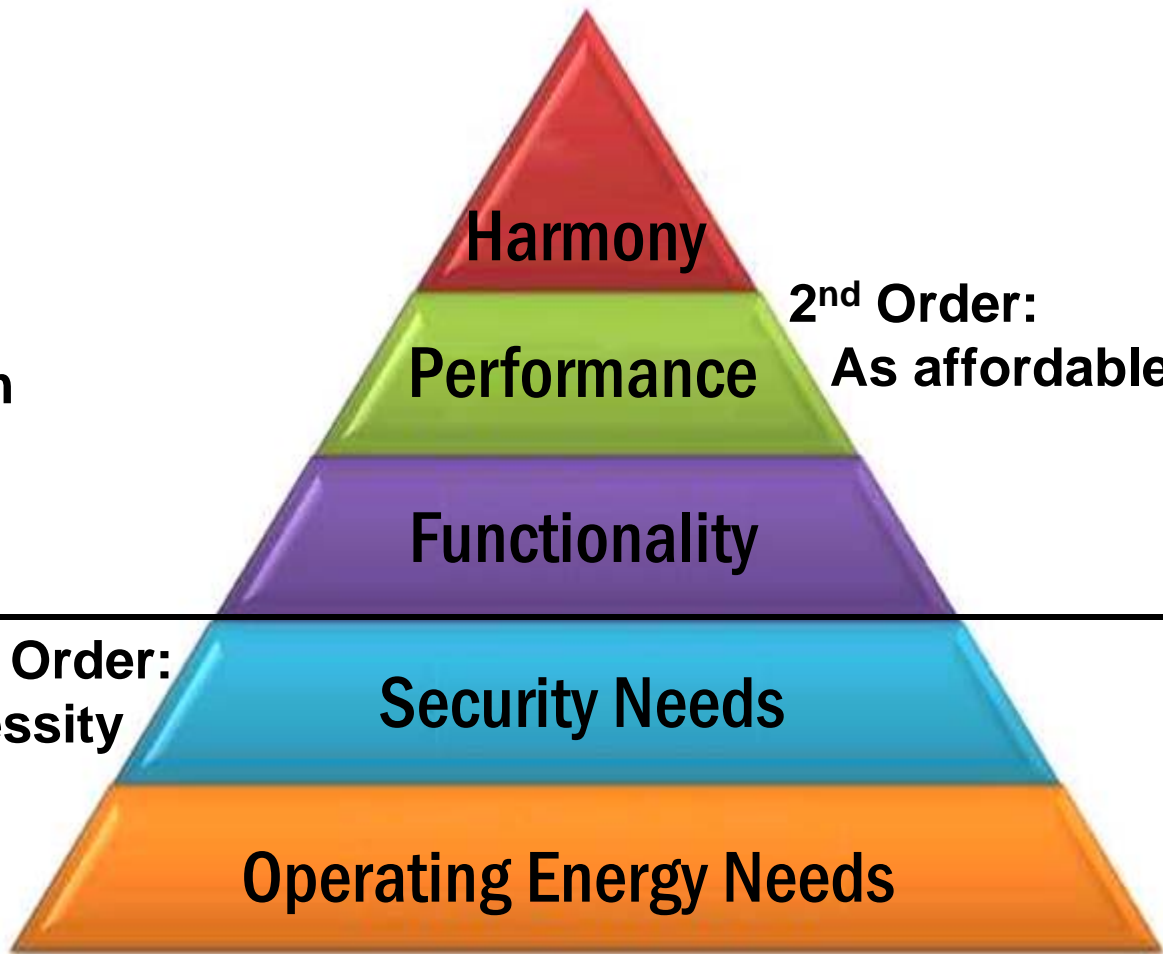
Its not about Cyber Security

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

The Cyber-Security problem cannot be fixed from within the cyber-world. (supply chain, insider threat, physical attacks, social attacks, user priorities, organizational priorities ...)

**1st Order:
Core necessity**

**2nd Order:
As affordable**

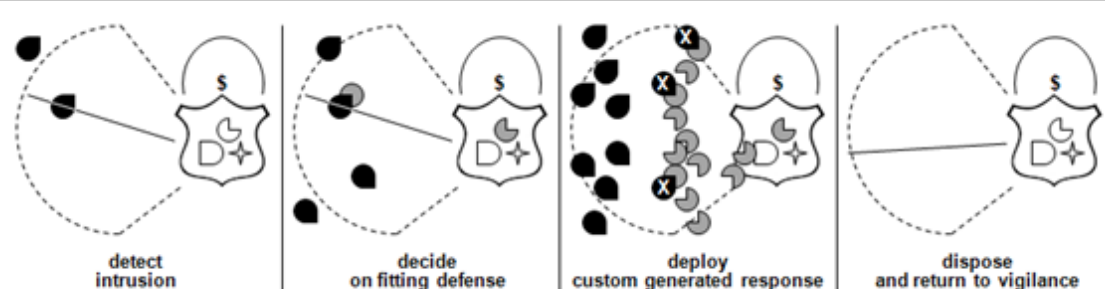


Mirror the Enemy



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.**

<p>Name: Dynamic Phalanx Defense</p>
<p>Context: a stationary or mobile asset subject to unpredictable swarm attacks.</p>
<p>Problem: Attackers can come in many and unpredictable forms, and in virtually unbounded quantities, with no advance warning. For instance, A <u>DDoS</u> attack on an Internet service node may be of many different types; an attack on a naval asset may be surface, undersea or air in many different varieties.</p>
<p>Forces: Resilience of service vs. cost of service. Comprehensive counter capability and capacity vs cost and disharmony of a broad standing counter force.</p>
<p>Solution: the ability to detect the threat and the nature of its attack, the ability to produce and deploy appropriate disposable counter-measures, the ability to deploy measure-for-measure and to stand down or dispose of deployed counter measures when the threat is vanquished.</p>
 <p style="text-align: center;">Aggressive shield waxes and wanes measure-for-measure in real time</p>
<p>Example: Artificial immune system – detection, selection, cloning and retirement applied to mobile network intrusion detection and repulsion. See (Edge et al. 2006, Zhang et al. 2008).</p>
<p>Example: Botnet denial of service defense – Instantly recruit an unbounded network of computers to shield a server from being overwhelmed by botnets. See (Dixon et al. 2008, Mahimkar et al. 2007).</p>
<p>Example: Just-in-time drone swarms – Load disposable drones with modular sensor and weapon choices, and deploy quantities as needed. See SWARM, <u>IITSA</u> discussion in (Hambling 2006).</p>
<p>Example: Plant chemical defense – Insect saliva triggers selective toxic gene expression and gas emissions that call in selective insect predators.,</p>
<p>Agility: Self organization grows and shrinks a counter swarm in measured response to an attack swarm. Adaptability selects appropriate counter-swarm agents from modular resources. Resilience is exhibited with expendable and replicable counter agents, and in continued operation of the protected asset, though perhaps at reduced performance. The process is harmonious with protected asset functionality as it is only activated upon detecting a threat, and then only in dynamic measure-for-measure as needed. [S-A-R-H]</p>
<p>References: (see reference section, only URL shown here, all accessed 30Nov09)</p> <ul style="list-style-type: none"> • (Dixon et al. 2008) www.cs.washington.edu/homes/ckd/phalanx.pdf. • (Edge et al. 2006) http://paper.ijcsns.org/07_book/200603/200603C08.pdf • (Hambling 2006) http://defensetech.org/2006/04/10/drone-swarm-for-maximum-harm/ • (Mahimkar et al. 2007) www.cs.utexas.edu/~yzhang/papers/dfence-nsdi07.pdf • (Wilkinson 2001) http://pubs.acs.org/cen/critter/plantsbugs.html • (Zhang et al. 2008) www.computer.org/portal/web/csdi/doi/10.1109/ICNC.2008.782

Example of a pattern description synopsis.

These descriptions are for path-finder patterns rather than well-known common-practice patterns, full understanding is either obtained from reading the referenced papers or from reading accompanying discussion pages.

Evolution and Innovation

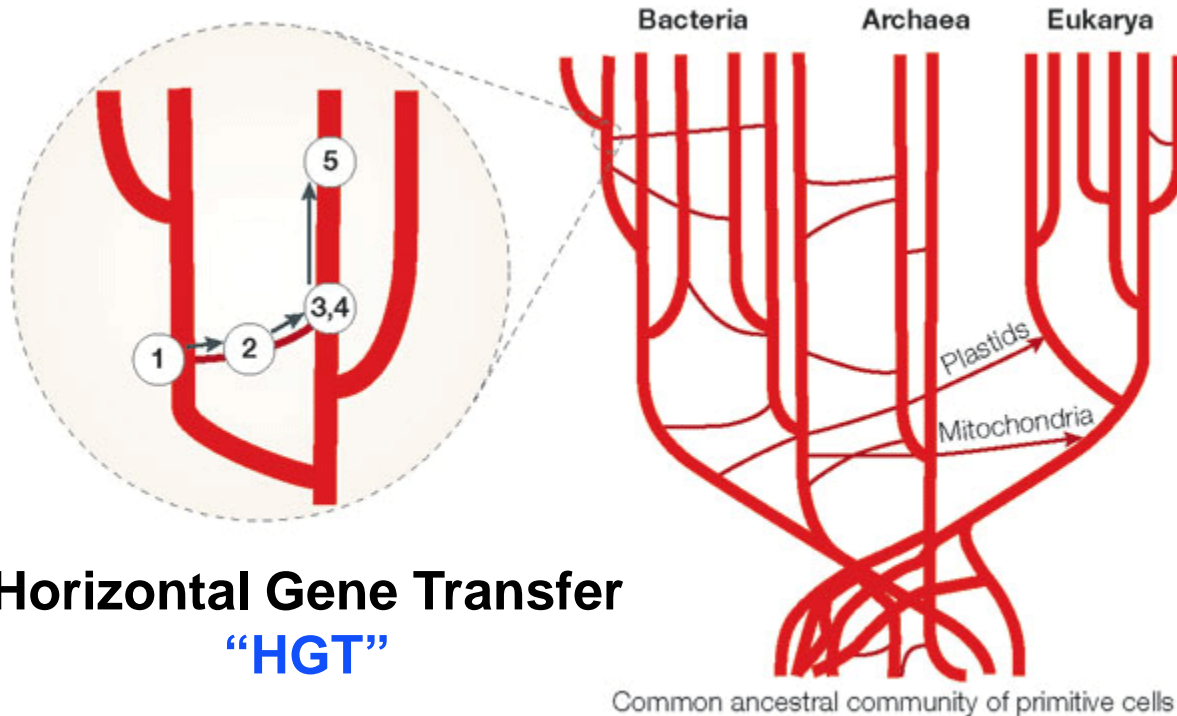
Woese, Carl. 2000. Interpreting the universal phylogenetic tree. PNAS. 97(15):8392-6. www.ncbi.nlm.nih.gov/pmc/articles/PMC26958/pdf/pq008392.pdf

“Vertically generated and horizontally acquired variation could be viewed as the yin and the yang of the evolutionary process.

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.”



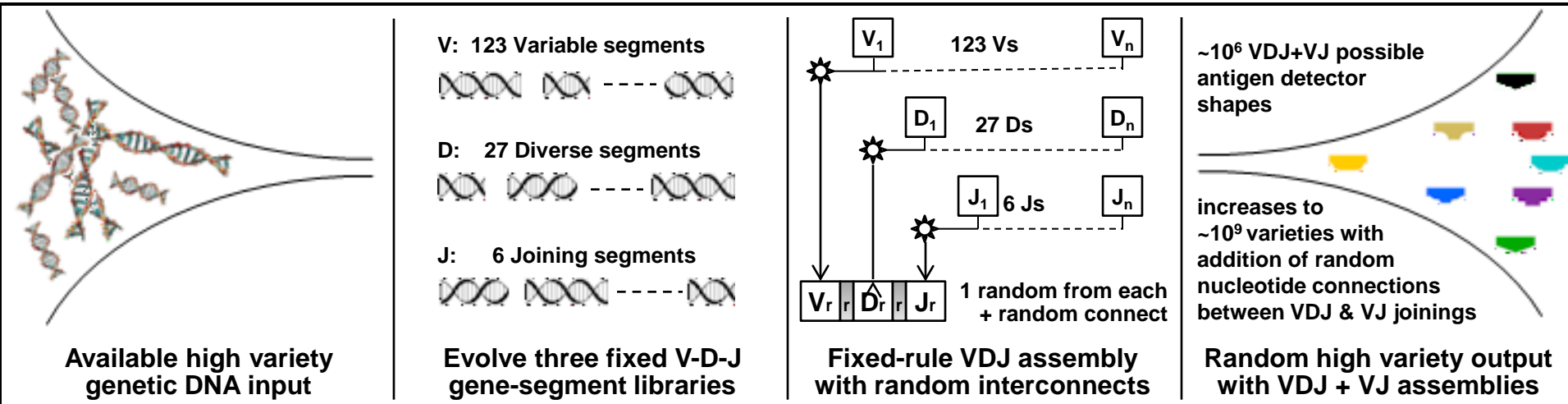
Copyright © 2005 Nature Publishing Group

Horizontal Gene Transfer
“HGT”

A continuum of 5 steps leading to the stable inheritance of a transferred gene in a new host.

Figure from: Smets, Barth F. and Tamar Barkay. 2005. Horizontal gene transfer: perspectives at a crossroads of scientific disciplines. *Nature Reviews Microbiology* 3, 675-678 (September 2005).

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



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

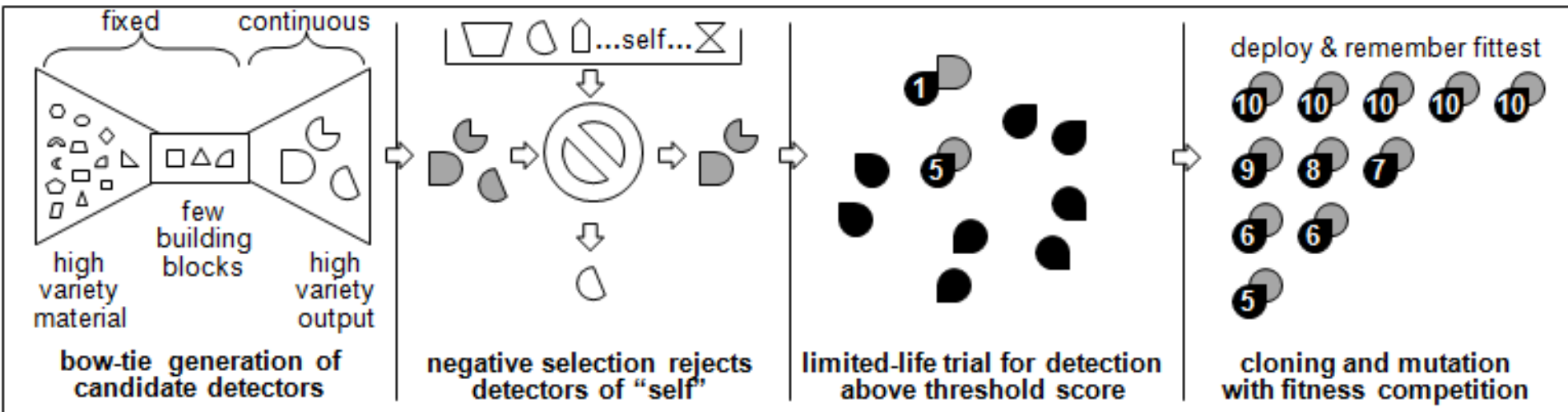
Context: Complex system with many diverse inputs and many diverse outputs, where outputs need to respond to many needs or innovate for many or unknown opportunities, and it is not practical to build unique one-to-one connections between inputs and outputs. Appropriate examples include common financial 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 (antigen epitopes) for unknown attacks and infections. A reactive example is a manufacturing line that constructs products for customers demanding custom capabilities.

Pattern: Proactive Search



Speculative generation and mutation of detectors recognizes new attacks like a biological immune system

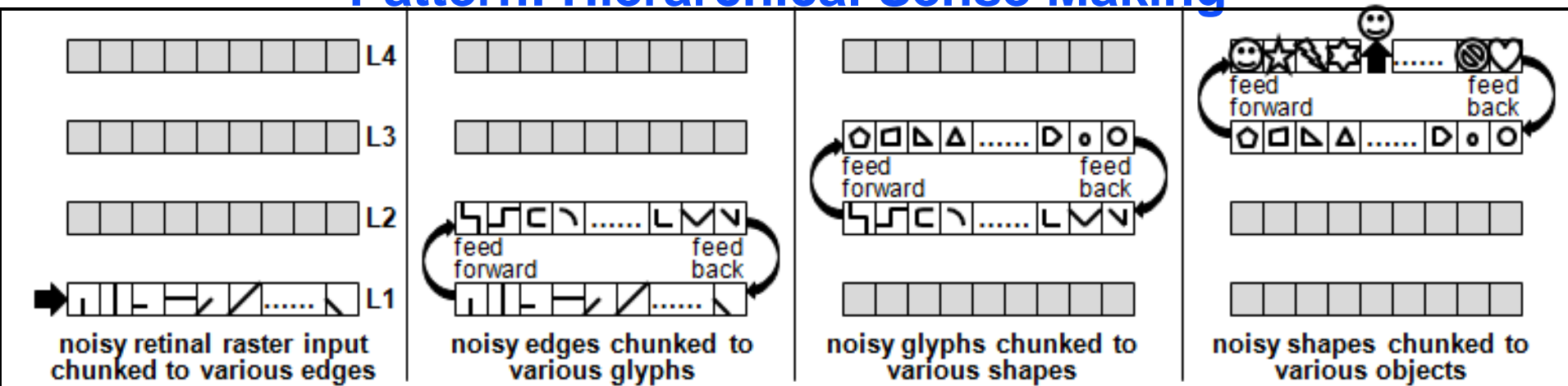
Context: A complex system or system-of-systems subject to attack and infection, with low tolerance for attack success and no tolerance for catastrophic infection success; with resilient remedial action capability when infection is detected. Appropriate examples include biological organisms, and cyber 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 detection of self.

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 Sense Making



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 vary 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, which is then 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 relatively small number of an infinite set of data-combination possibilities, but as aggregation proceeds through multiple levels, complex data abstractions and recognitions are enabled.

Pattern: Horizontal Meme Transfer

<p>multi-agent systems biological organisms open systems everyday life communities guerillas enterprise insects markets society hackers animals games</p> <p>patterns from many dynamic system domains</p>	<p>hierarchical sense making horizontal gene transfer peer monitoring genetic algorithm quorum sensing immune system coevolution mutual aid etc, etc</p> <p>relevant candidate patterns for situational awareness</p>	<ol style="list-style-type: none"> 1. immune system speculative detector generator and self-test 2. immune system time-limited test of speculative detectors 3. genetic algorithm detector improvement for successful hits 4. community coevolution of effective detectors situation-specific selected adaptations 	<pre> graph TD RC([random creation]) --> ST([self test]) ST --> TR([trial]) TR --> DE([death]) TR --> HI([hit]) HI --> IMP([improve]) IMP --> MEM([memory]) MEM --> HI HI -.-> OHG([other host generators]) OHG -.-> HI subgraph CIG [collaborative intrusion detector generators] RC ST TR DE HI IMP MEM end </pre>
---	--	---	---

Massive shared generation of intrusion detectors for evolving resilient-network vigilance

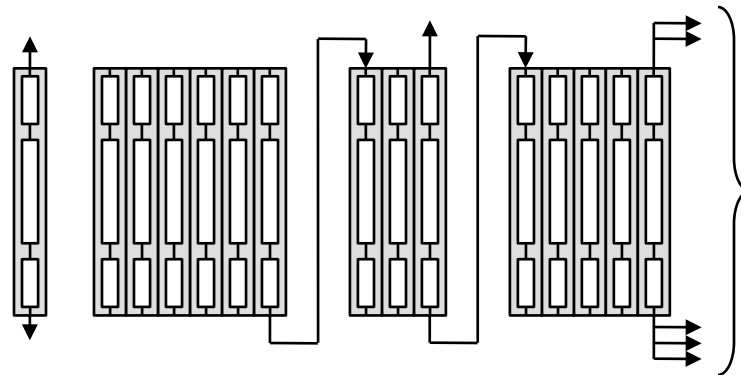
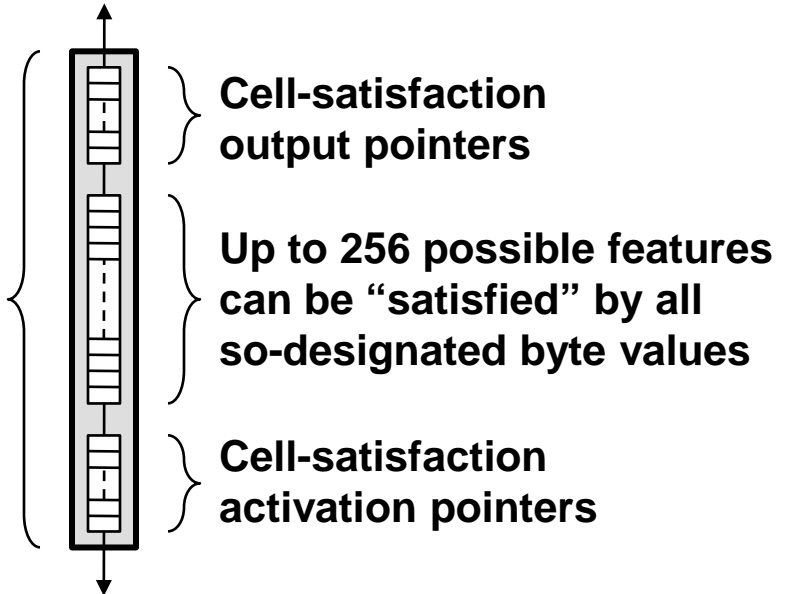
<p>Name: Horizontal Meme Transfer (adapting patterns from other domains)</p>
<p>Context: Systemic innovation and evolution.</p>
<p>Problem: A need for improved system survivability, either reactive, proactive, or both.</p>
<p>Forces: Evolution of innovation vs. evolution of robustness.</p>
<p>Solution: Find relevant patterns in other domains and adapt them to the perceived threats and opportunities of the system of interest.</p>

Reconfigurable Pattern Processor

Reusable Cells Reconfigurable in a Scalable Architecture

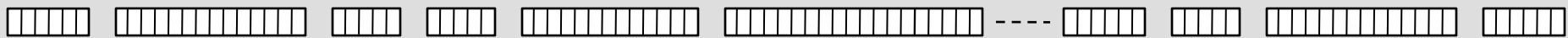
Independent detection cell:
content addressable
by current input byte

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



Individual detection cells are configured
into *detectors* by linking activation
pointers.

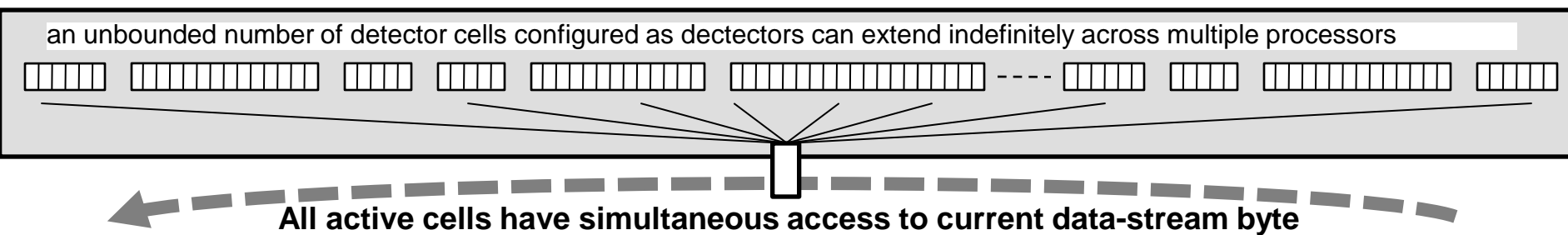
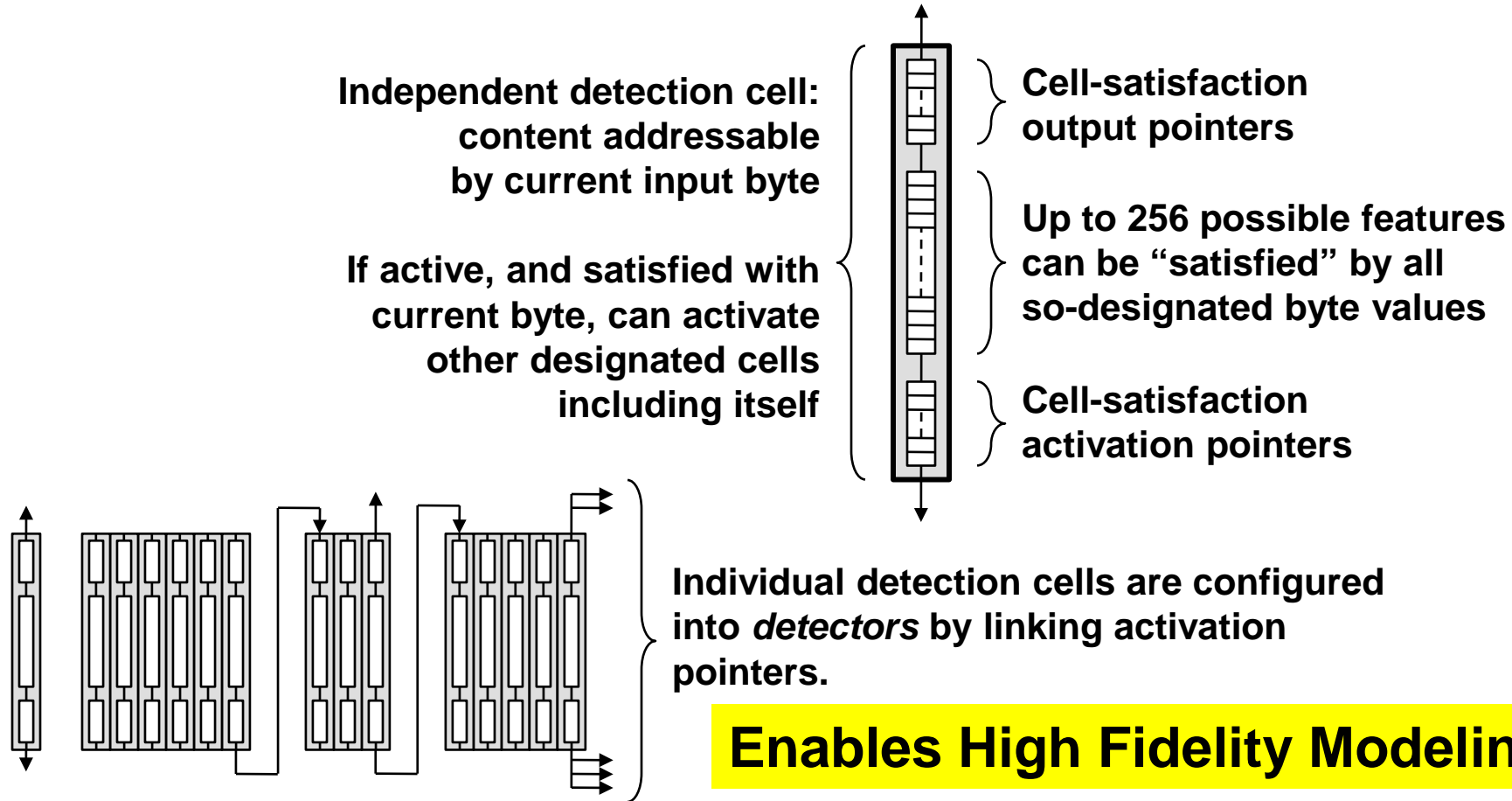
an unbounded number of detector cells configured as detectors can extend indefinitely across multiple processors



All active cells have simultaneous access to current data-stream byte

Reconfigurable Pattern Processor

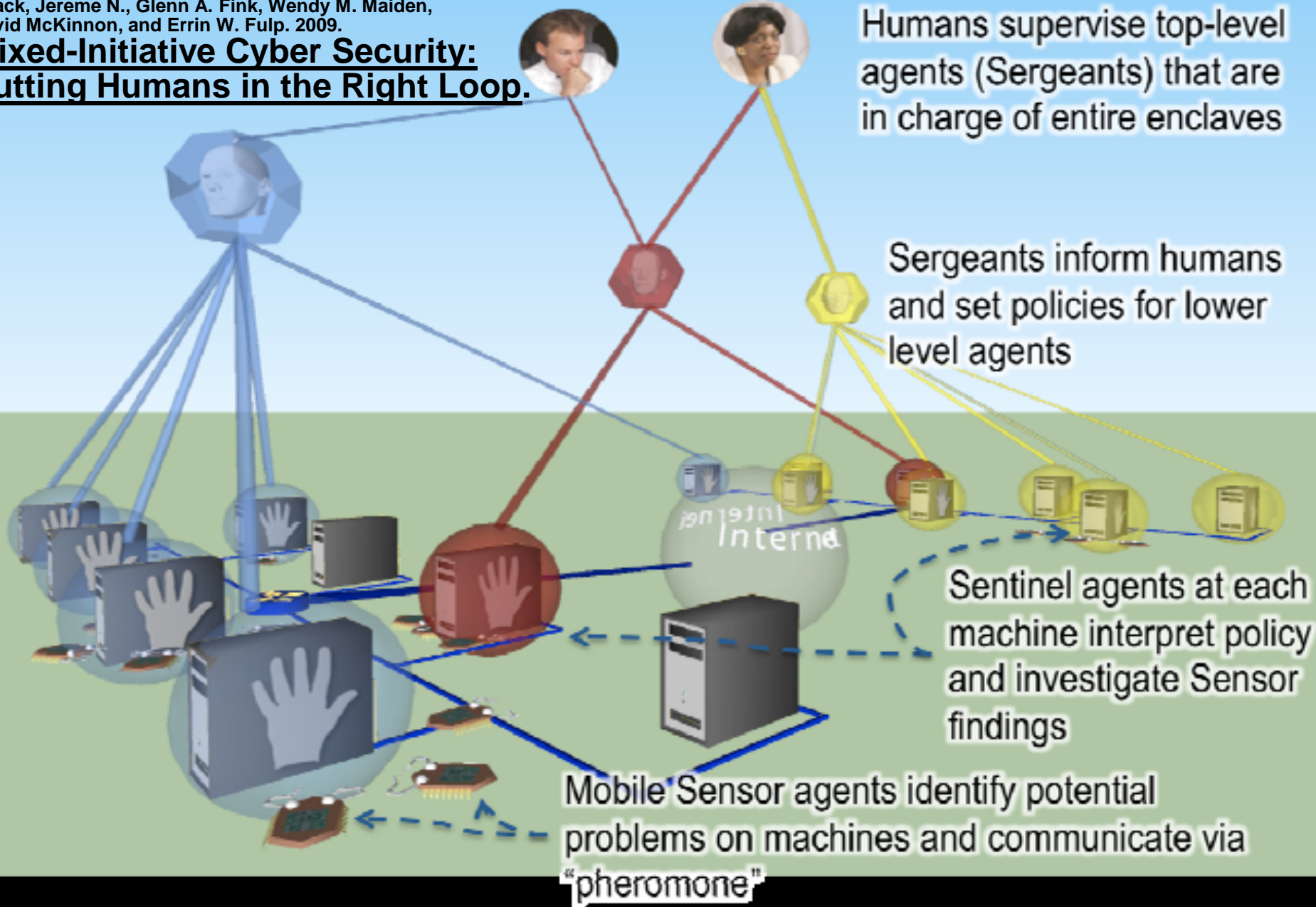
Reusable Cells Reconfigurable in a Scalable Architecture



Example: Hierarchical Management

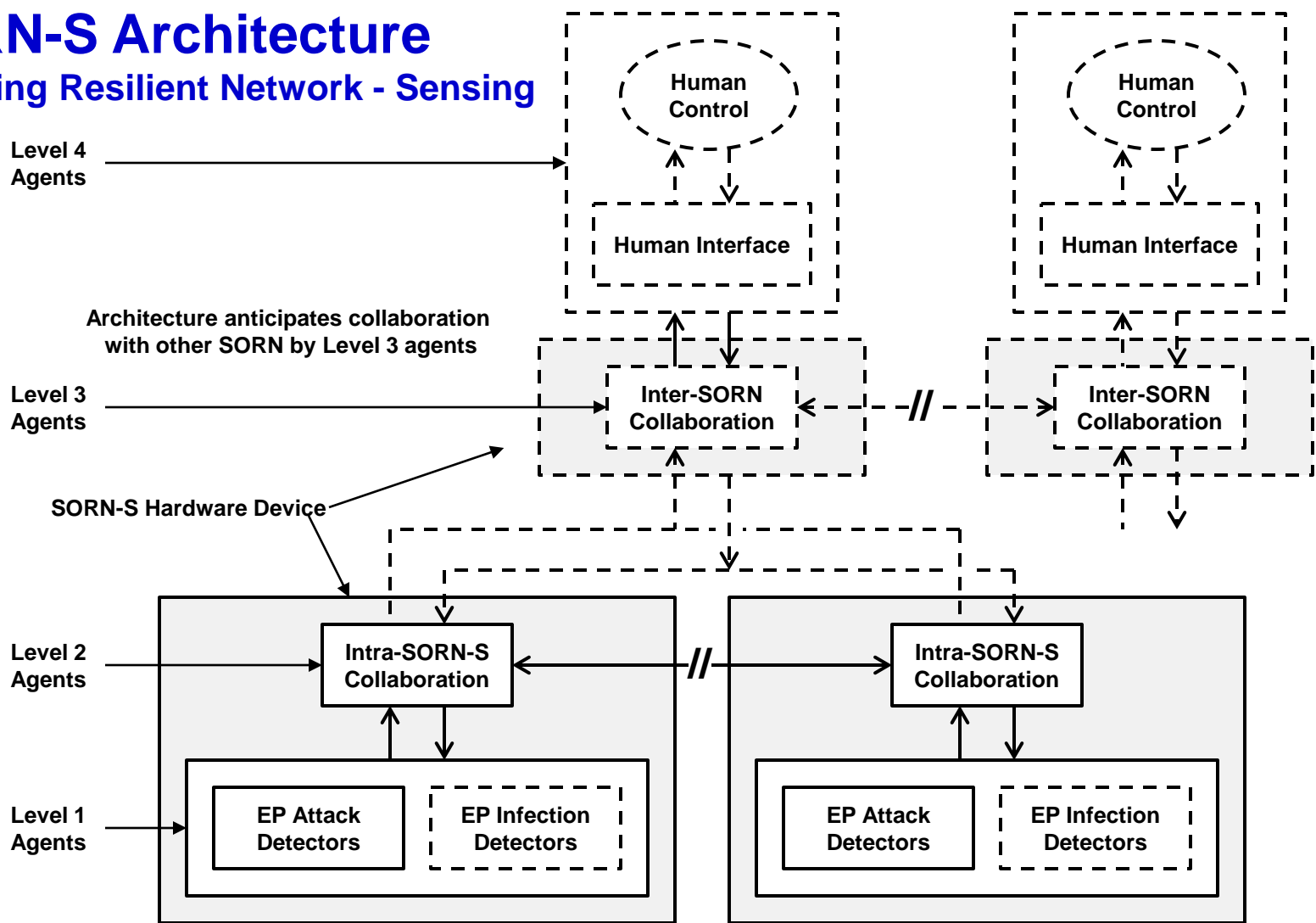
Haack, Jereme N., Glenn A. Fink, Wendy M. Maiden,
David McKinnon, and Errin W. Fulp. 2009.

Mixed-Initiative Cyber Security: Putting Humans in the Right Loop.



SORN-S Architecture

Self Organizing Resilient Network - Sensing



Multi-level architecture refines sensory input through learning and sensemaking hierarchy, supports remedial action agents (human/automated) with succinct relevant information.

Notes:

- For general all-level hierarchical network-agent architecture general concept see (Haack 2009)
- For hierarchical feed-forward/backward pattern learning, prediction, and sense-making see (George 2009).
- For all-level hierarchical learning of causal patterns spread as time-sequence events see (Hawkins 2010).

Level 1 & 2 Agent: Detector Creation & Learning Architecture

General L1 detector life cycle: creation, false-positive testing, deployment efficacy or termination, mutation improvement, and long-term memory.

1. Candidate fuzzy detector semi-randomly created.
2. Tolerization period tests immature candidates for false-positive matches.
3. Mature & naïve candidates put into time limited service.
4. Activated (B-cell) candidates wait for co-stimulation (by T-cells) to ensure “improvement” didn’t produce auto-reactive result, non-activated & non-co-stimulated candidates die when time limit ends.
5. Highest scoring co-stimulated candidates are remembered for time-limited long term.
6. Co-stimulated candidates are cloned with structured mutations, looking for improved (higher) activation scores.
7. Level 2 Agent insertion of activated candidates from other end-points, and Level 2 Agent distribution of activated candidates to other end points.

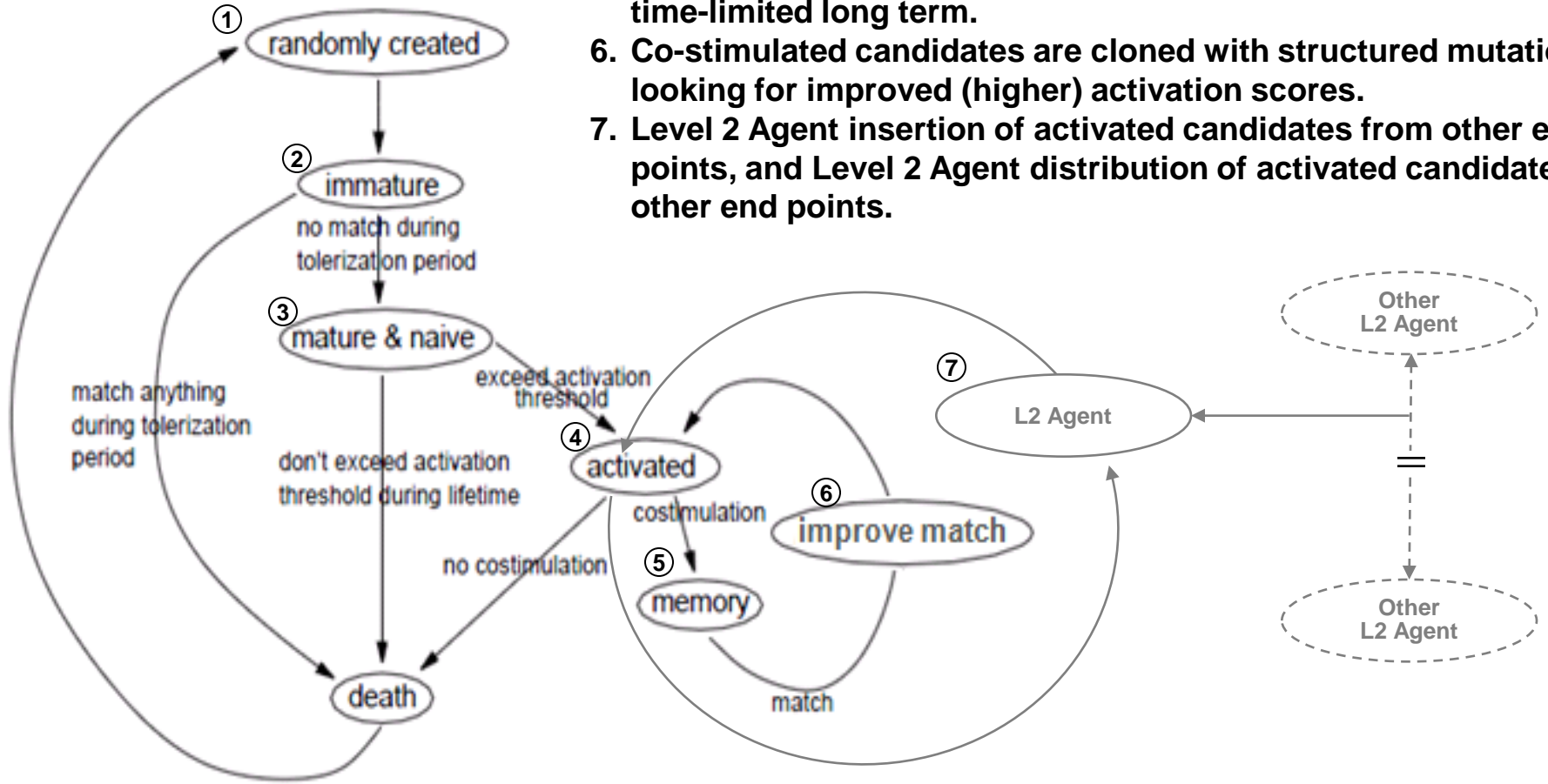


Diagram modified from (Hofmeyr 2000).

SPECIAL FORUM

on NEXT-GENERATION SECURITY at ITNG 2011

International Conference on Information Technology - New Generations (ITNG)
WWW.ITNG.INFO, Las Vegas, Nevada, April 11-13, 2011

Toward Next-Generation Security: Self-Organizing Perspectives, Principles, and Patterns

A new approach to systems security is in order. The innovation of determined adversaries adapts and evolves faster than reactive defense. Looked upon as self-organizing exploitation systems, adversaries are diverse in nature and allegiance, but their strength is rooted in common characteristics: self-organizing, adaptive, evolving, proactive, resilient, and single-minded purpose. In a word, the adversary is agile. The strength of adversary success stems from common roots. Roots that should be respected and mirrored for parity in new proactive strategy. Critical mass appears to exist, but is working narrowly-focused goals in relative isolation. This call is for a preliminary catalyzing event – one that might inspire a broad based community loosely defined by a shared sense of common goal and principles for next generation security strategy.

Papers are sought that will articulate perspectives, principles and patterns appropriate for a self-organizing system-of-systems security strategy, featuring systemic innovation and evolution enabled by holistic system architecture, and likely leveraging multi-agent community concepts.

Opportunities...

ITNG April Forum – Catalyzing a Community

**Contribute a pattern to the growing collection
(and/or Join INCOSE SSE WG)**

**Write a 200 word essay for INCOSE Insight July 2011
(Theme: Systems of Systems and Self Organizing Security)**

**Be a SORN-S Project Reviewer
(Get a work-in-progress project brief, act as soft Red Team)**

**Be on the Technology Application Tour
(Q2 2011 pattern processor capability/applications briefings)**

SO-SoS scares people

- but they are all around us
- and the adversary thrives on it

SysE, SecE and Decision Makers don't communicate

Only SysE can enable next gen SecE: SO-SoS

We need a common language and vision

- for SysE, SecE, and Decision Makers

Patterns reflected from common understandings

- solve communication problem
- solve scary problem
- brings shared vision into focus

References

- Armstrong, Robert C. and Jackson R. Mayo. 2009. Leveraging Complexity in Software for Cybersecurity. CIIRW 2009, April 13-15, Oakridge TN. http://portal.acm.org/beta/ft_gateway.cfm?id=1558643&type=pdf&CFID=82493696&CFTOKEN=93605741
- Carlson, Jean and John Doyle. 2000. Highly Optimized Tolerance: Robustness and Design in Complex Systems, *Physical Review Letters* 84 (11): 2529–2532, 13 March.
- Carlson, Jean and John Doyle. 2002. Complexity and Robustness. PNAS 99: 2538–2545, 19 February.
- Csete, Marie and John Doyle. 2010. Bow Ties, Metabolism and Disease, TRENDS in Biotechnology 22(9), September 2004. www.cds.caltech.edu/~doyle/CmplxNets/Trends.pdf.
- Dixon, Colin, Anderson, Thomas and Krishnamurthy, Arvind, Phalanx: Withstanding Multimillion-Node Botnets, NSDI'08: Proceedings of the 5th USENIX Symposium on Networked Systems Design and Implementation, April 2008.
- Dove, Rick. 2009. Embedding Agile Security in System Architecture. *Insight* 12 (2): 14-17. International Council on Systems Engineering, July. www.parshift.com/Files/PsiDocs/Pap090701In cose-Embedding Agile Security In System Architecture.pdf
- Dove, Rick. 2010. Pattern Qualifications and Examples of Next-Generation Agile System-Security Strategies, IEEE International Carnahan Conference on Security Technology (ICCST), San Jose, CA, USA, 5-8 October.
- Dove, Rick. 2010. Self Organizing Resilient Network Sensing Using Patterns from Natural and Adversarial Processes, working paper, www.parshift.com/Files/PsiDocs/PatternsForResilientNetworkSensing&Sensemaking.pdf
- Dove, Rick. 2010. Illuminating Next Generation Agile Security Patterns. SERC Security Research Roadmap Workshop, March 31-April 1, Washington, D.C. www.parshift.com/Files/PsiDocs/Pap100331SERC-IlluminatingNextGenAgileSecurityPatterns.pdf
- Forrest, S., Perelson, A. S., Allen, L., and Cherukuri, R., Self-Nonself Discrimination in a Computer, In Proceedings IEEE Symposium on Research in Security and Privacy, Oakland, CA., May 16–18, 1994.
- Forrest, S., Balthrop, J., Glickman, M. and Ackley, D.. K. Park and W. Willins Eds. *The Internet as a Large-Scale Complex System*, Oxford University Press, 2005.
- Haack, Jereme N., Glenn A. Fink, Wendy M. Maiden, David McKinnon, and Errin W. Fulp. 2009. Mixed-Initiative Cyber Security: Putting Humans in the Right Loop. www.cs.wfu.edu/~fulp/Papers/mims09f.pdf
- S. Hofmeyr and S. Forrest. 2000. "Architecture for an Artificial Immune System." *Evolutionary Computation* 7(1), Morgan-Kaufmann, San Francisco, CA, pp. 1289-1296. http://cs.unm.edu/~forrest/publications/hofmeyr_forrest.pdf
- Mahimkar, A. , Dange, J., Shmatikov, V., Vin, H. and Zhang, Y., dFence: Transparent Network-Based Denial of Service Mitigation, in Proceedings of 4th USENIX Symposium on Networked Systems Design and Implementation (NSDI 2007), Cambridge, MA, April, 2007.
- Smets, Barth F. and Tamar Barkay. 2005. Horizontal gene transfer: perspectives at a crossroads of scientific disciplines. *Nature Reviews Microbiology* 3, 675-678 (September 2005).
- Wilkinson, Sophie, Plants to Bugs: Buzz Off!, *Chemical and Engineering News*, June 30, 2001.
- Woese, Carl. 2000. Interpreting the universal phylogenetic tree. PNAS. 97(15):8392-6. www.ncbi.nlm.nih.gov/pmc/articles/PMC26958/pdf/pq008392.pdf
- Zhang, C., Zhang, J., Liu, S., and Liu, Y., Network Intrusion Active Defense Model Based on Artificial Immune System. Fourth International Conference on Natural Computation, Jinan, China, October 18-20, 2008.