SYSTEMS ENGINEERING
Research Center

The Systems Engineering University Affiliated Research Center

Systems Security Workshop

March 31 – April 1, 2010

On Next Generation Patterns of Agile System Security

Rick Dove

www.parshift.com/Files/PsiDocs/Pap100331SERC-IlluminatingNextGenAgileSecurityPatterns.pdf

End Item: Systems Security Engineering

SYSTEMS ENGINEERING
Research Center

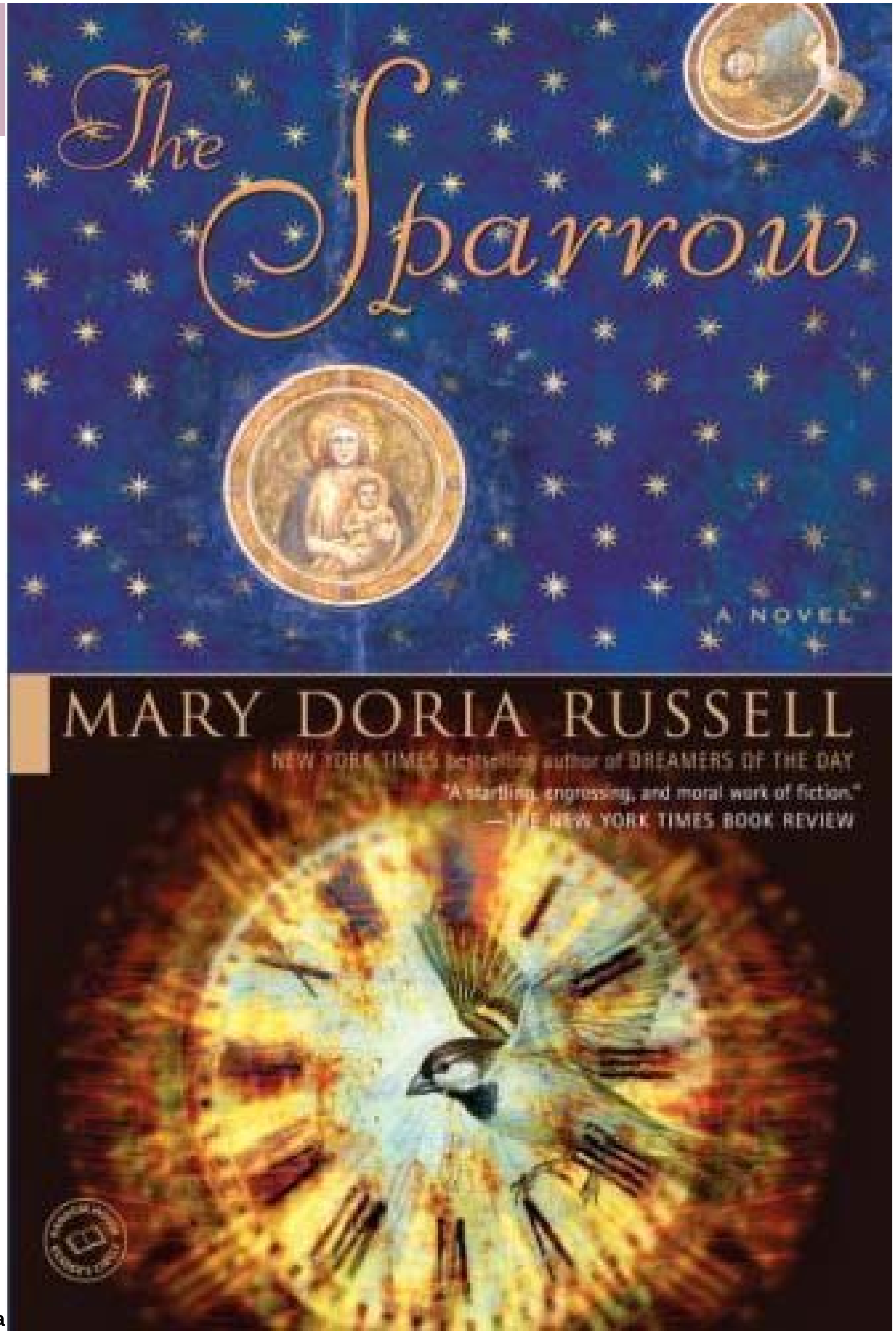
Academic, publishing anthropologist.
Converted from Catholic to Jew.
First fiction book (1997).
Wrote to resolve personal questions.

Story:

- **Life discovered on Mars.**
- **Missionary Jesuits fund space trip.**
- **One priest, the rest are scientists.**
- **First contact.**

To their horror, they discover…

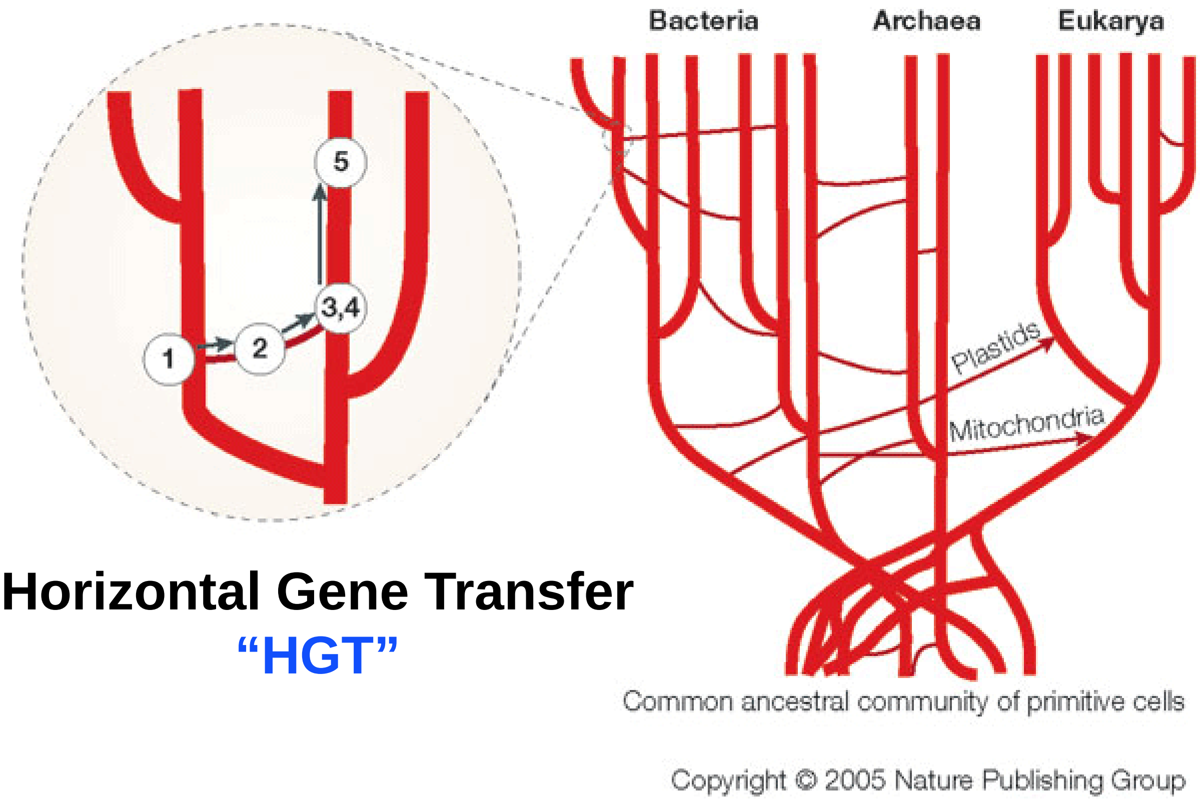
- **Two sentient intelligent life forms.**
- **One predator, the other pray.**
- **Both comfortable with status quo.**
- **Predators lead co-evolution.**



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.



Horizontal Gene Transfer

"HGT"

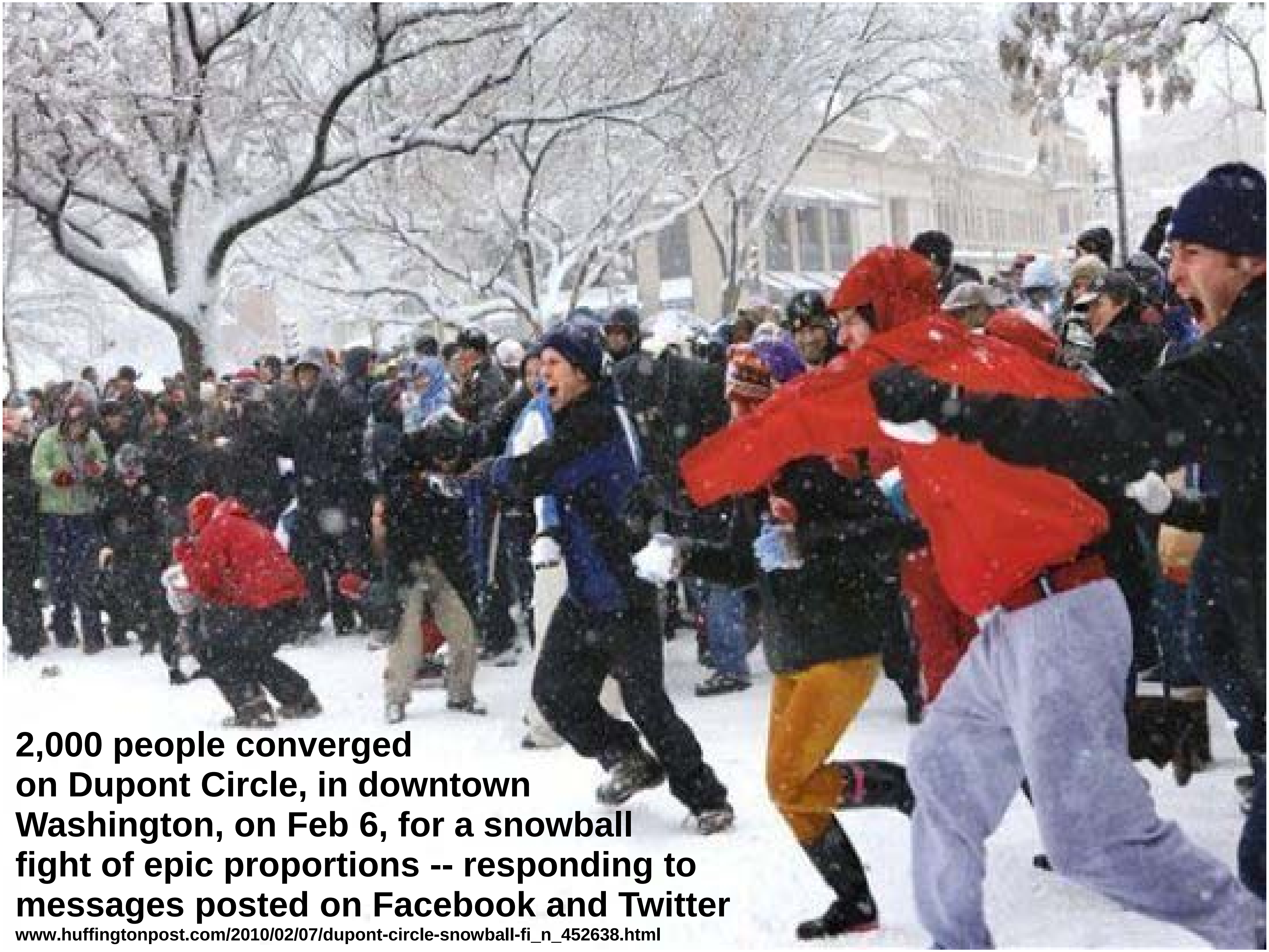
A continuum of 5 steps leading to the stable inheritance of a transferred gene in a new host.

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).

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."



2,000 people converged on Dupont Circle, in downtown Washington, on Feb 6, 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

March 24, 2010, www.nytimes.com/2010/03/25/us/25mobs.html?hp

March 20: Philadelphia Text-Message Flash Mob

2003 performance-art flash-mob inventor surprised with violent turn

HGT = Adversarial Advantage

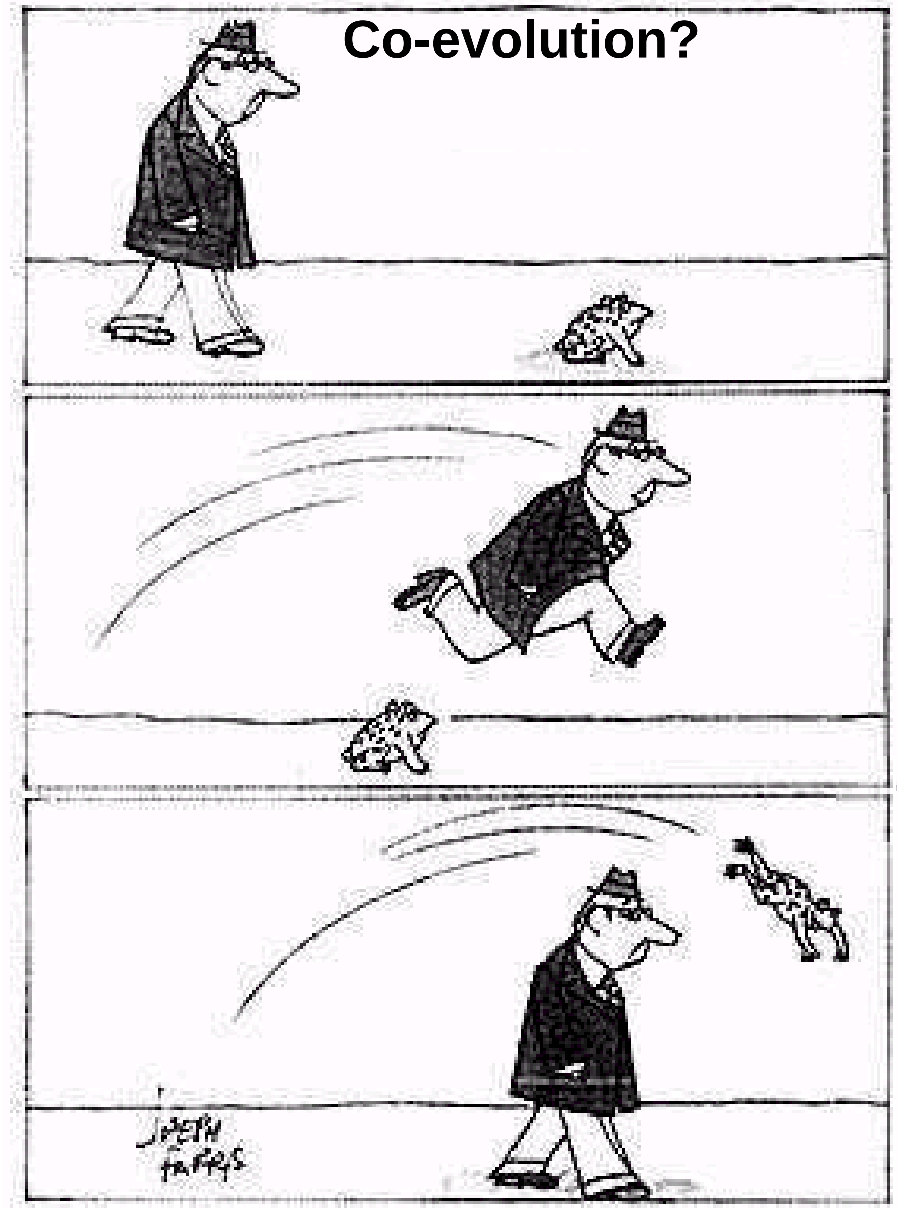
Architecture:

- **Multi-agent**
- **Loosely coupled**
- **Self organizing**
- **Systems-of-systems**

Behavior:

- **Swarm intelligence**
- **Tight learning loops**
- **Fast evolution**
- **Dedicated intent**

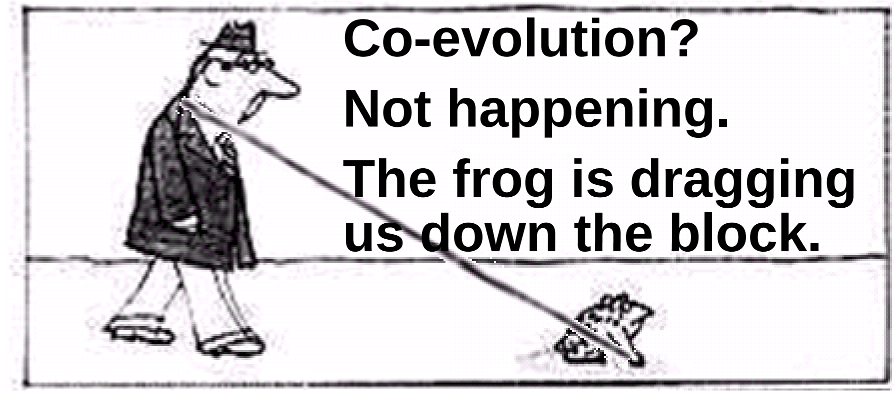
We are not in an arms race – we haven't engaged.



HGT = Adversarial Advantage

Architecture:

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



Behavior:

- Swarm intelligence
- Tight learning loops
- Fast evolution
- Dedicated intent

We are not in an arms race – we haven't engaged.

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.

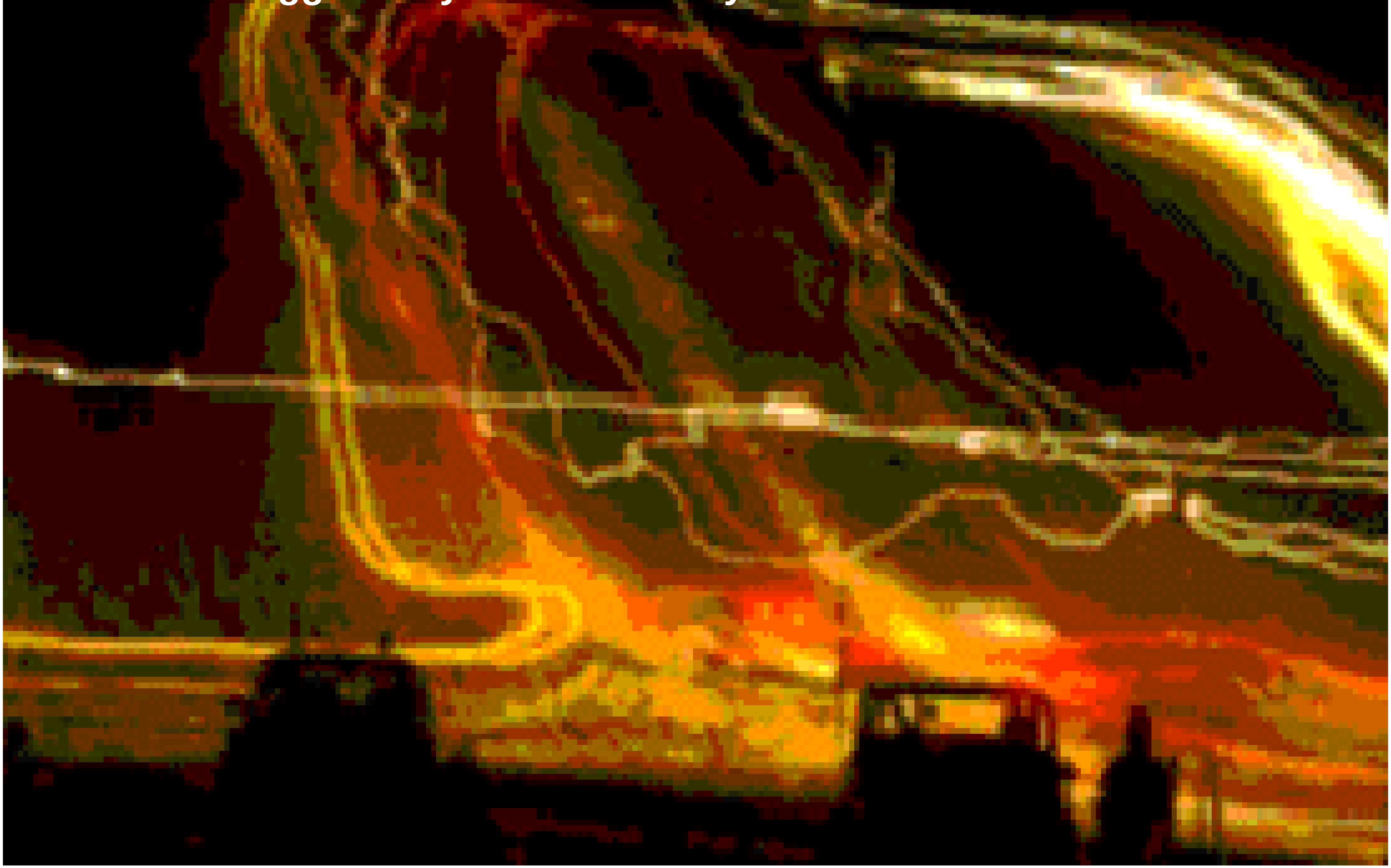
[P] Proactively innovative – acting preemptively, perhaps unpredictably, to gain advantage.

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

Community: The Internet Storm Center

http://isc.sans.org/about.html

Hundreds of volunteer global experts monitoring in shifts.
Suspected incident recruits data from 100,000 subscribers.
Action then triggered by informed analysis.



SYSTEMS ENGINEERING
Research Center

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

Its Not About Cyber Security (more condiments for the hot dogs at the picnic)

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, HMT & HTM, …)

Maslow's Hierarchy of Needs

2nd Order: As affordable

1st Order: Core necessity

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

Pattern Format

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.

SYSTEMS ENGINEERING
Research Center

Figure 2. Example of a pattern description synopsis. As these descriptions are for path-finder patterns rather than of well-known common-practice patterns, full understanding is either obtained from reading the referenced papers or from reading accompanying discussion pages.

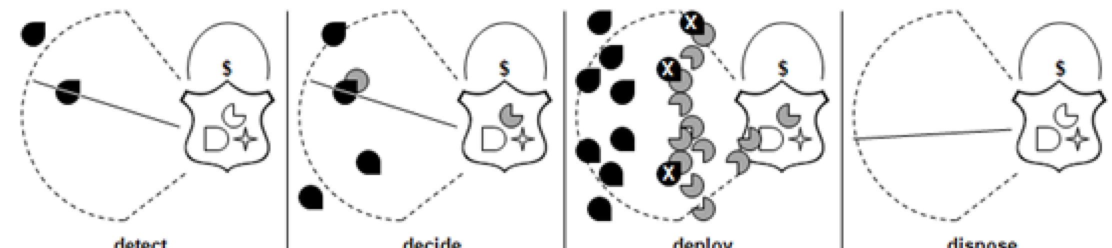
Name: Dynamic Phalanx Defense

Context: a stationary or mobile asset subject to unpredictable swarm attacks.

Problem: Attackers can come in many and unpredictable forms, and in virtually unbounded quantities, with no advance warning. For instance, A DDoS 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.

Forces: Resilience of service vs. cost of service. Comprehensive counter capability and capacity vs cost and disharmony of a broad standing counter force.

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.



Aggressive shield waxes and wanes measure-for-measure in real time

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).

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).

Example: Just-in-time drone swarms – Load disposable drones with modular sensor and weapon choices, and deploy quantities as needed. See SWARM, JITSA discussion in (Hambling 2006).

Example: Plant chemical defense – Insect saliva triggers selective toxic gene expression and gas emissions that call in selective insect predators.,

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]

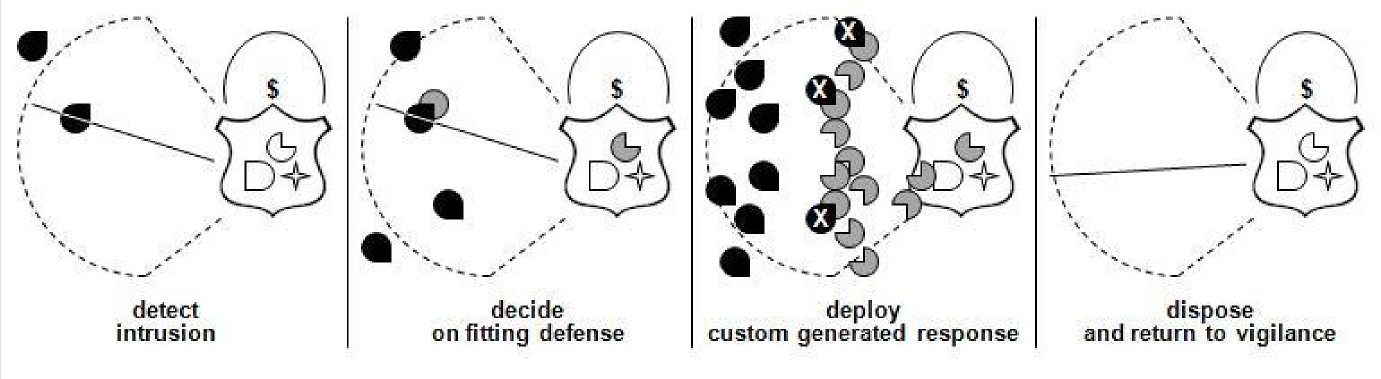
References: (see reference section, only URL shown here, all accessed 30Nov09)

- (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/csdl/doi/10.1109/ICNC.2008.782

Dynamic Phalanx Defense 1/3

Name:	Dynamic Phalanx Defense
Context:	a stationary or mobile asset subject to unpredictable swarm attacks.
Problem:	Attackers can come in many and unpredictable forms, and in virtually unbounded quantities, with no advance warning. For instance, A DDoS 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.
Forces:	Resilience of service vs. cost of service. Comprehensive counter capability and capacity vs cost and disharmony of a broad standing counter force.

Dynamic Phalanx Defense[2/3]

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.
Graphic:	
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]

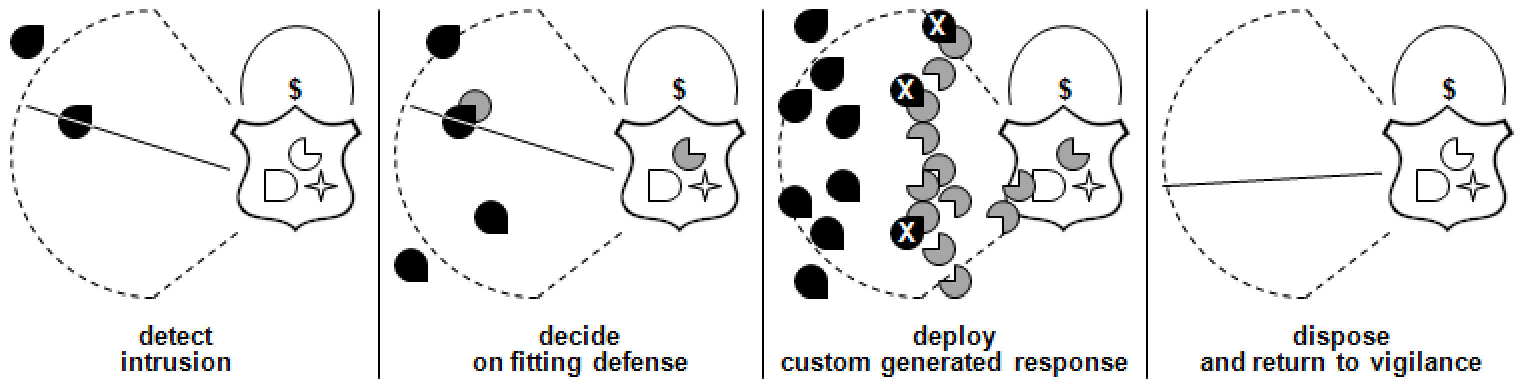
SYSTEMS ENGINEERING Research Center

Dynamic Phalanx Defense[3/3]

Examples:	**Botnet denial of service defense –** Use a scalable network of computers to shield a server from being overwhelmed by botnets. Server sends requests to friendly computers to retrieve requests at its own pace. Phalanx: Withstanding Multimillion-Node Botnets (Dixon et al. 2008) dFence: Transparent Network-based Denial of Service Mitigation (Mahimkar et al. 2007)
	Just-in-time defensive drone swarms – Sense and respond automatically to launch drone swarms against ambushes and flash threats to warfighting assets. Drone Swarm for Maximum Harm (Hambling 2006)
	Artificial immune system – detection, selection, cloning and retirement applied to mobile network intrusion detection and repulsion. Multi-objective Mobile Network Anomaly Intrusion (Edge et al. 2006) Network Intrusion Active Defense Model Based on Artificial Immune System (Zhang et al. 2008) .
	Plant chemical defense – Insect saliva triggers selective toxic gene expression and gas emissions that call in selective insect predators. Plants Use Volatile Signaling Compounds to Fend Off Attack and Possibly Warn Nearby Plants. Plants to Bugs: Buzz Off! (Wilkinson 2001)

SYSTEMS ENGINEERING
Research Center

Dynamic Phalanx Defense



Aggressive shield waxes and wanes measure-for-measure in real time

---

Example: Artificial immune system – detection, selection, cloning and retirement applied to mobile network intrusion detection and repulsion. See (Zhang et al. 2008, Edge et al. 2006).

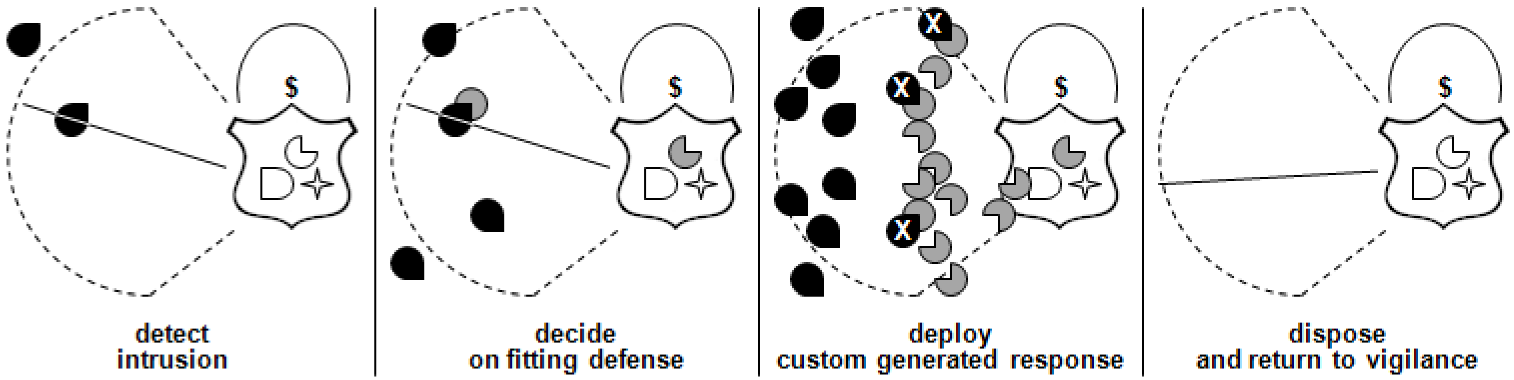
Example: Botnet denial of service defense – Instantly recruit an unbounded network of computers to shield a server from being overwhelmed by botnets. See (Dixon et al. 2008, Mahimkar et al. 2007).

Example: Just-in-time drone swarms – Load disposable drones with modular sensor and weapon choices, and deploy quantities as needed. See SWARM, JITSA discussion in (Hambling 2006).

Example: Plants – Use volatile signaling compounds to fend off attack, activate neighbor plants to do the same, and call in predators. See (Wilkinson, 2001).

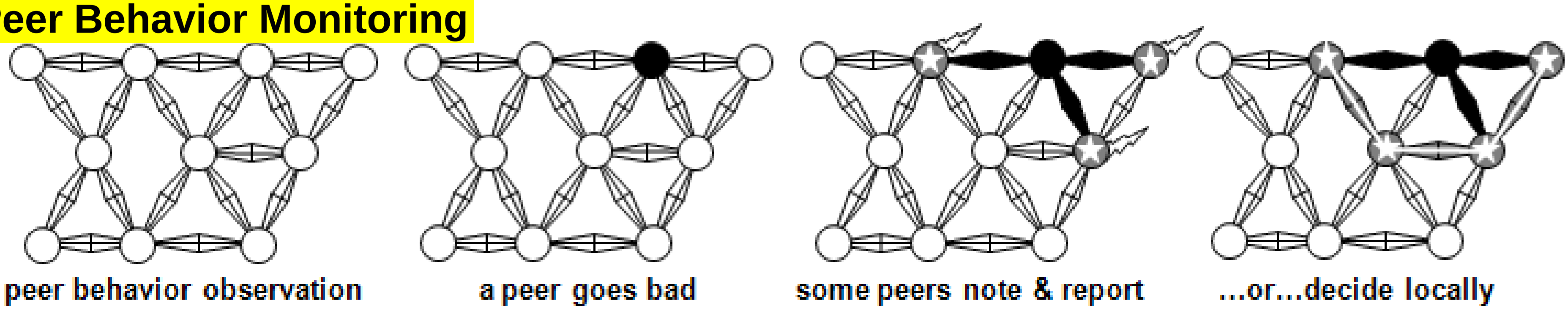
Above are systemically self-organized – here are some human directed examples
- **NATO**
- **Internet Storm Center**
- **Fire department mutual aid**
- **Incident response coalitions (Khurana 2009)**

Dynamic Phalanx Defense



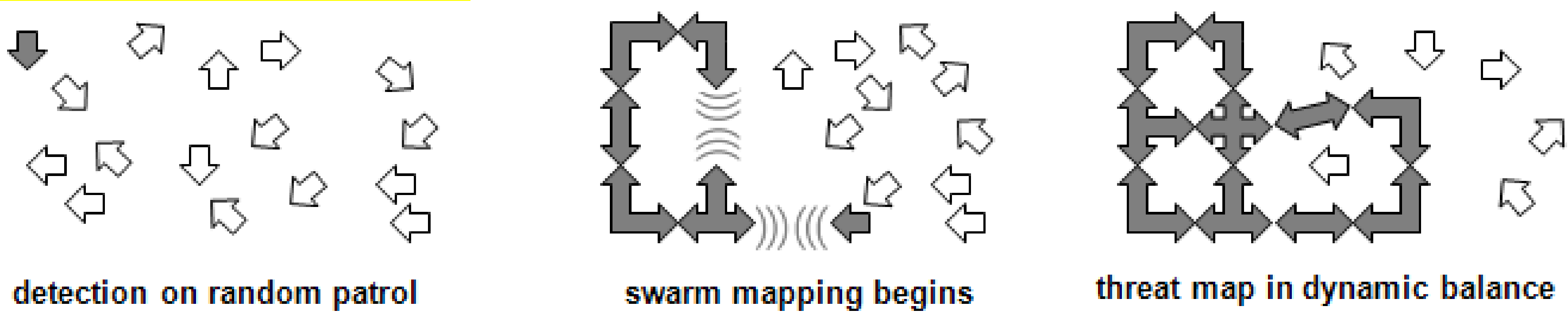
Aggressive shield waxes and wanes measure-for-measure in real time

Peer Behavior Monitoring



Peers monitor for aberrant behavior and tattle or decide locally

Swarming Threat Sensors

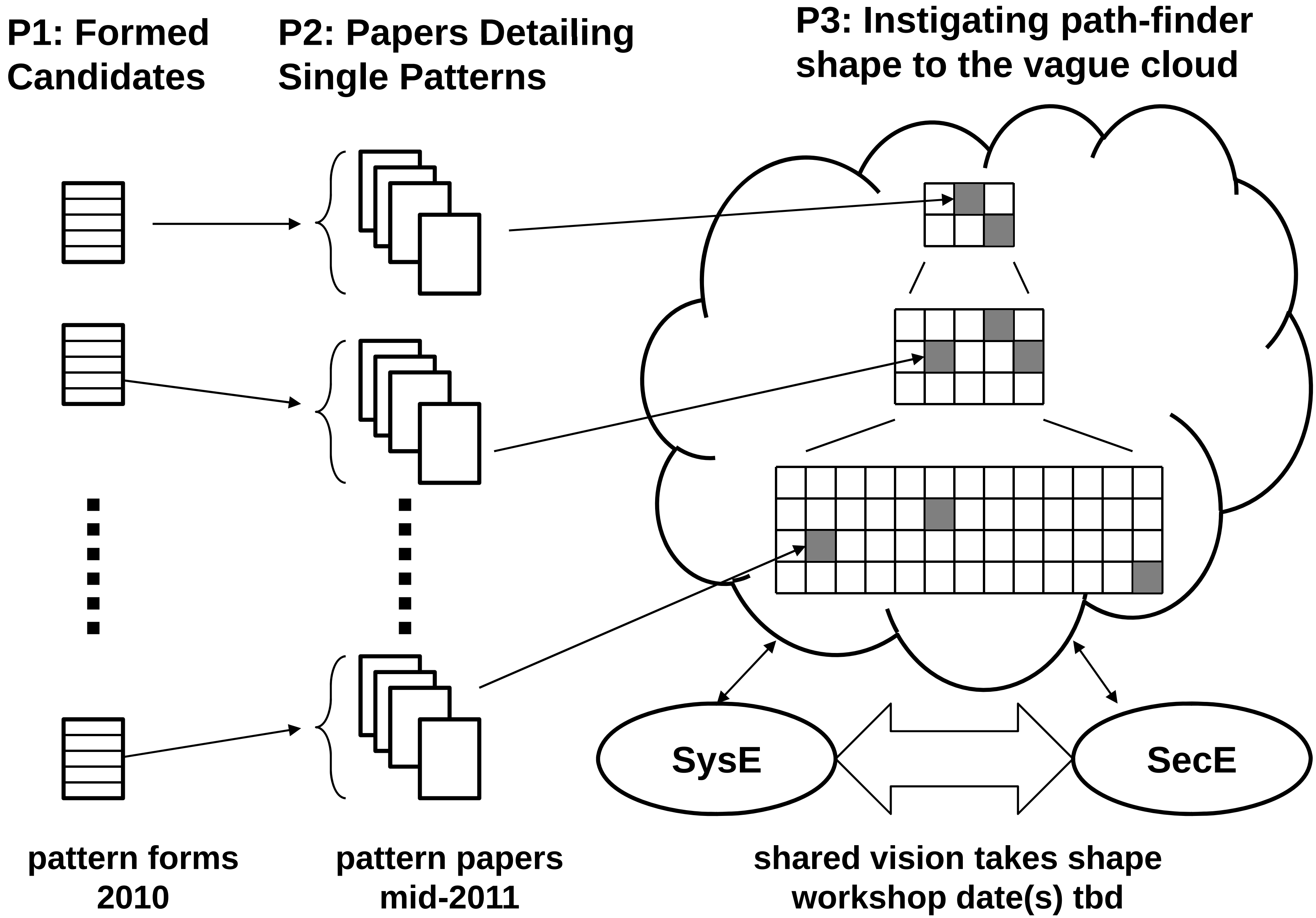


Swarm convergence seeks optimal sensor distribution to monitor detected threat

Path Finder Pattern Project

Systems Security Engineering Working Group - INCOSE

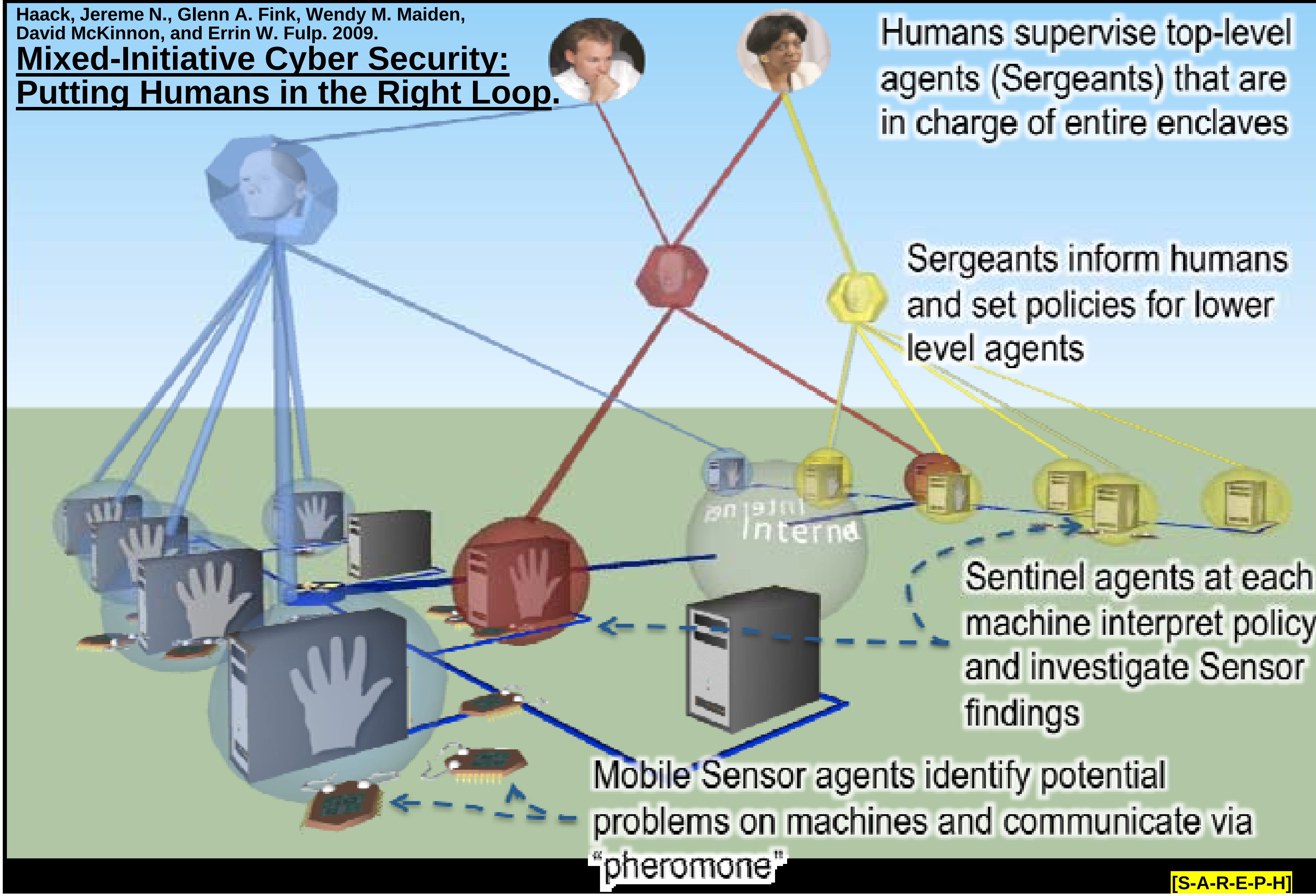
SYSTEMS ENGINEERING Research Center



www.parshift.com/Files/PsiDocs/Pap100101Insight-BuckStopsHere.pdf
www.parshift.com/Files/PsiDocs/Pap080401Insight-SecurityManifesto.pdf

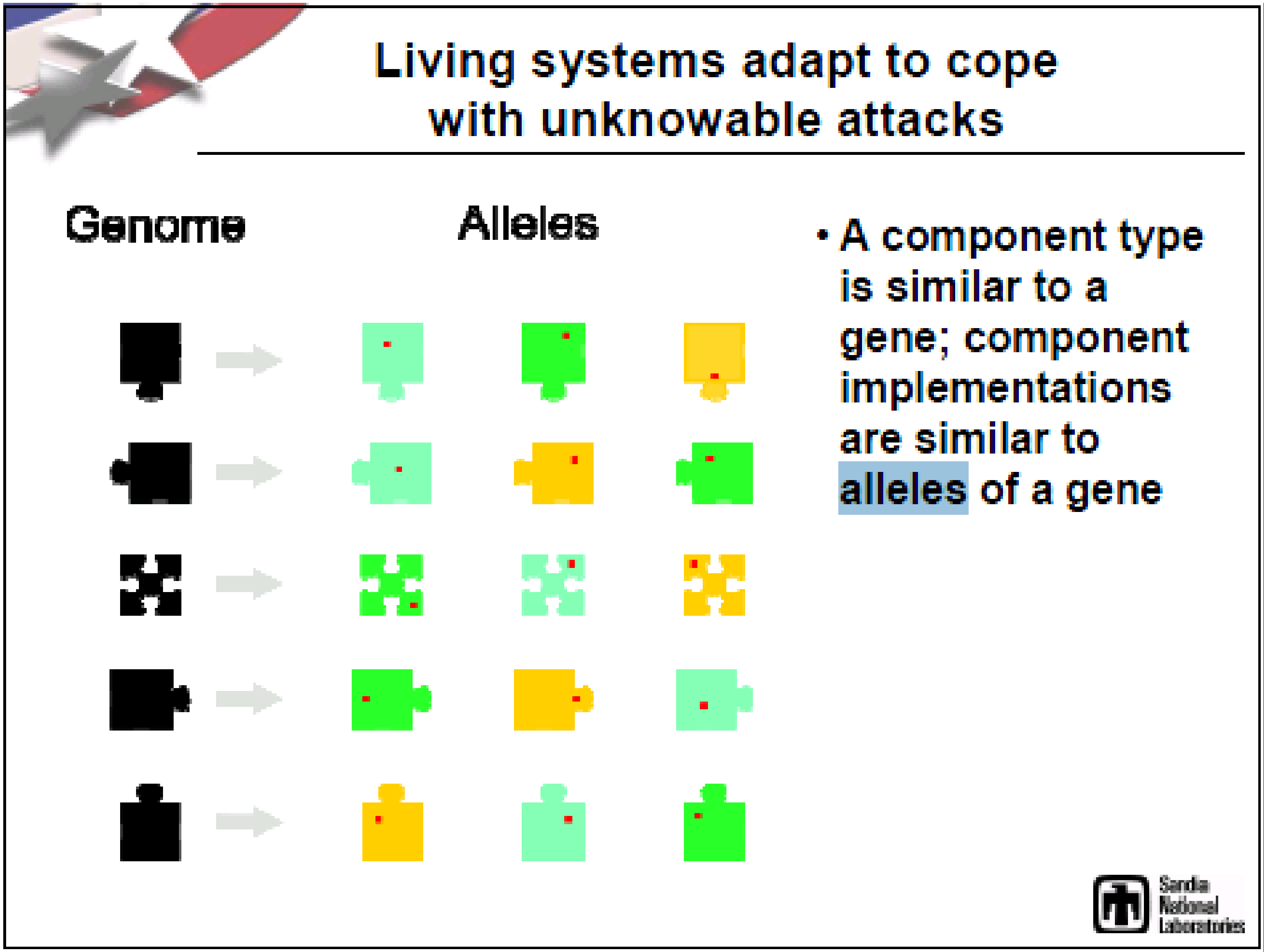
Cortical Processor Pattern: HTM
(Hierarchical Temporal Memory)

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.**



SYSTEMS ENGINEERING Research Center

Pattern: Component-Equivalent Diversity



Critical programs have multiple versions composed of component variants, with different vulnerabilities.

Output comparisons identify the one(s) in disagreement and possibly hacked.

Genetic algorithm (or other method) kills that variant and generates a new one, w/o the same vulnerability.

Robert C. Armstrong and Jackson R. Mayo. 2009. Leveraging Complexity in Software for Cybersecurity. CSIIRW 2009, April 13-15, Oakridge TN. http://portal.acm.org/beta/ft_gateway.cfm?id=1558643&type=pdf&CFID=82493696&CFTOKEN=93605741

Wrap

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

SYSTEMS ENGINEERING
Research Center

Horizontal Meme Transfer (HMT)

A prime and necessary pattern for innovative evolution of security.

The pattern that explains the research project:
find patterns across disciplines.

Rapid Innovation and Constant Evolution is the Secret Sauce.

The Comprehensive National Cybersecurity Initiative,
http://www.whitehouse.gov/sites/default/files/cybersecurity.pdf

Initiative #9

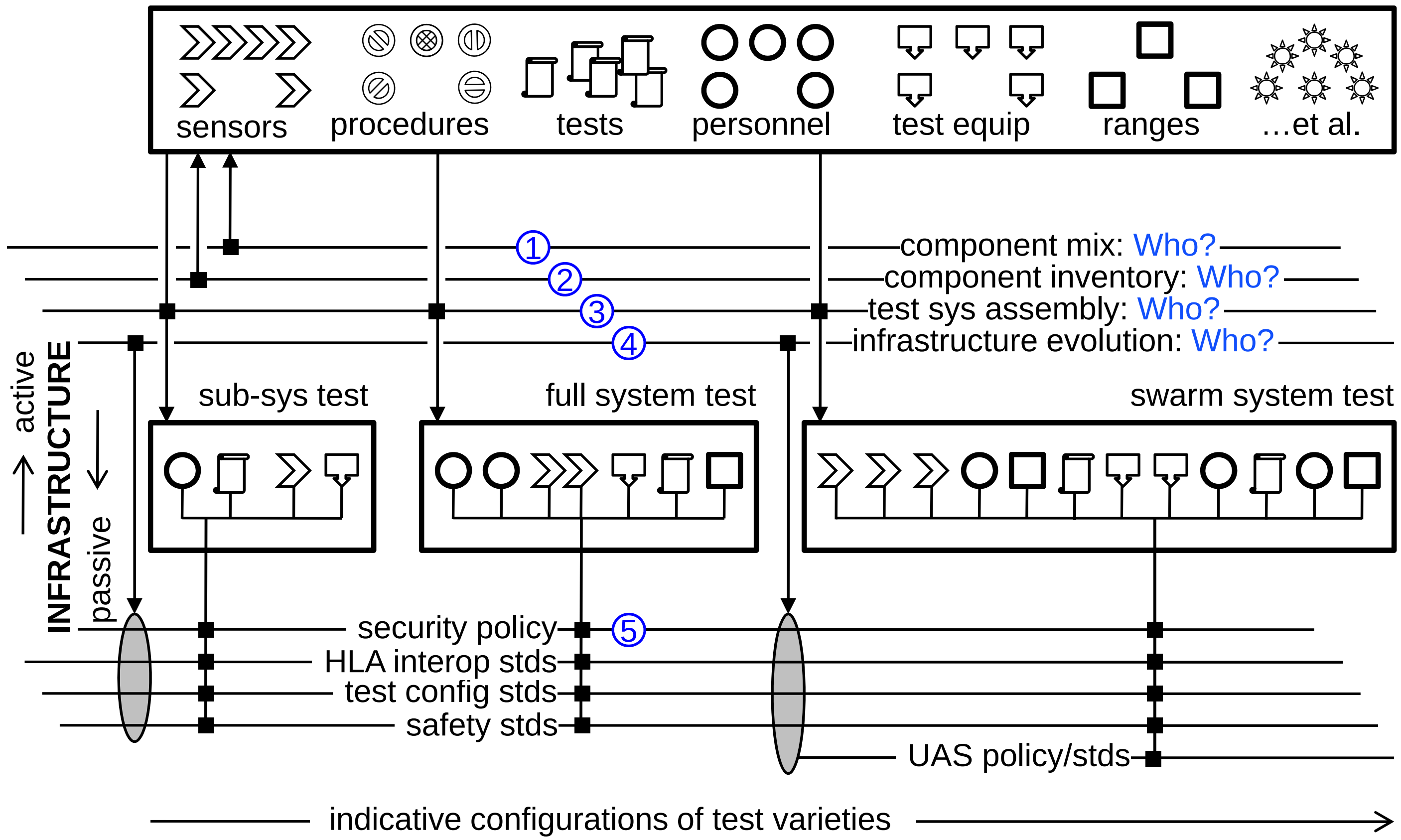
"Define and develop enduring "leap-ahead" technology, strategies, and programs. One goal of the CNCI is to develop technologies that provide increases in cybersecurity by orders of magnitude above current systems and which can be deployed within 5 to 10 years."

SO-SoS Fundamental Architecture

www.parshift.com/Files/PsiDocs/Pap090701Incose-EmbeddingAgileSecurityInSystemArchitecture.pdf

Multi-Range Weapons Testing System – UAST

(highly stylized architectural concept diagram)



As an emergent property security does not come in a separate box, e.g., personnel are security trained, equipment is self-secure.

Four active responsibilities, each with embedded security personnel as integrated collaborative team members.

Test system assembly is constrained by test configuration standards informed by security policy.

Security policy informs all other passive infrastructure standards, and evolves simultaneously with each.

Figure 3. Security is embedded in architecture at points 1-5. Additionally, encapsulated components have internal security distrustful of other components in general, ideally a fractal image of this architecture.

SYSTEMS ENGINEERING Research Center

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

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/Pap090701Incose-EmbeddingAgileSecurityInSystemArchitecture.pdf

Dove, Rick and Laura Shirey. 2010. On Discovery and Display of Agile Security Patterns. Conference on Systems Engineering Research, Stevens Institute of Technology, Hoboken, NJ, March 17-19. www.parshift.com/Files/PsiDocs/Pap100317Cser-OnDiscoveryAndDisplayOfAgileSecurityPatterns.pdf

Dove, Rick. 2010. Agile Security – Self-Organizing Co-Evolution. Working Paper. www.parshift.com/Files/PsiDocs/Pap100226-AgileSecuritySelfOrganizingCoEvolution-ExtAbst.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

Edge, Kenneth S., Gary B. Lamont, and Richard A. Raines, Multi-Objective Mobile Network Anomaly Intrusion, International Journal of Computer Science and Network Security, 6(3b):187-192, March, 2006.

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.

Hambling, Dave, Drone Swarm for Maximum Harm, Defense Tech. April 10, 2006.

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

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.

Myers, David, Play and Punishment: The Sad and Curious Case of Twixt, In Proceedings of The [Player] Conference, August 26-29, Copenhagen, Denmark, 2008.

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.