

# Attacking the Growing System Security Gap –The Frontier of Systems Engineering–

## INCOSE System Security Engineering Working Group Project Briefing

April 14, 2010

INCOSE Enchantment Chapter  
Rick Dove, SSE-WG Chair

**End Item: Systems Security Engineering**

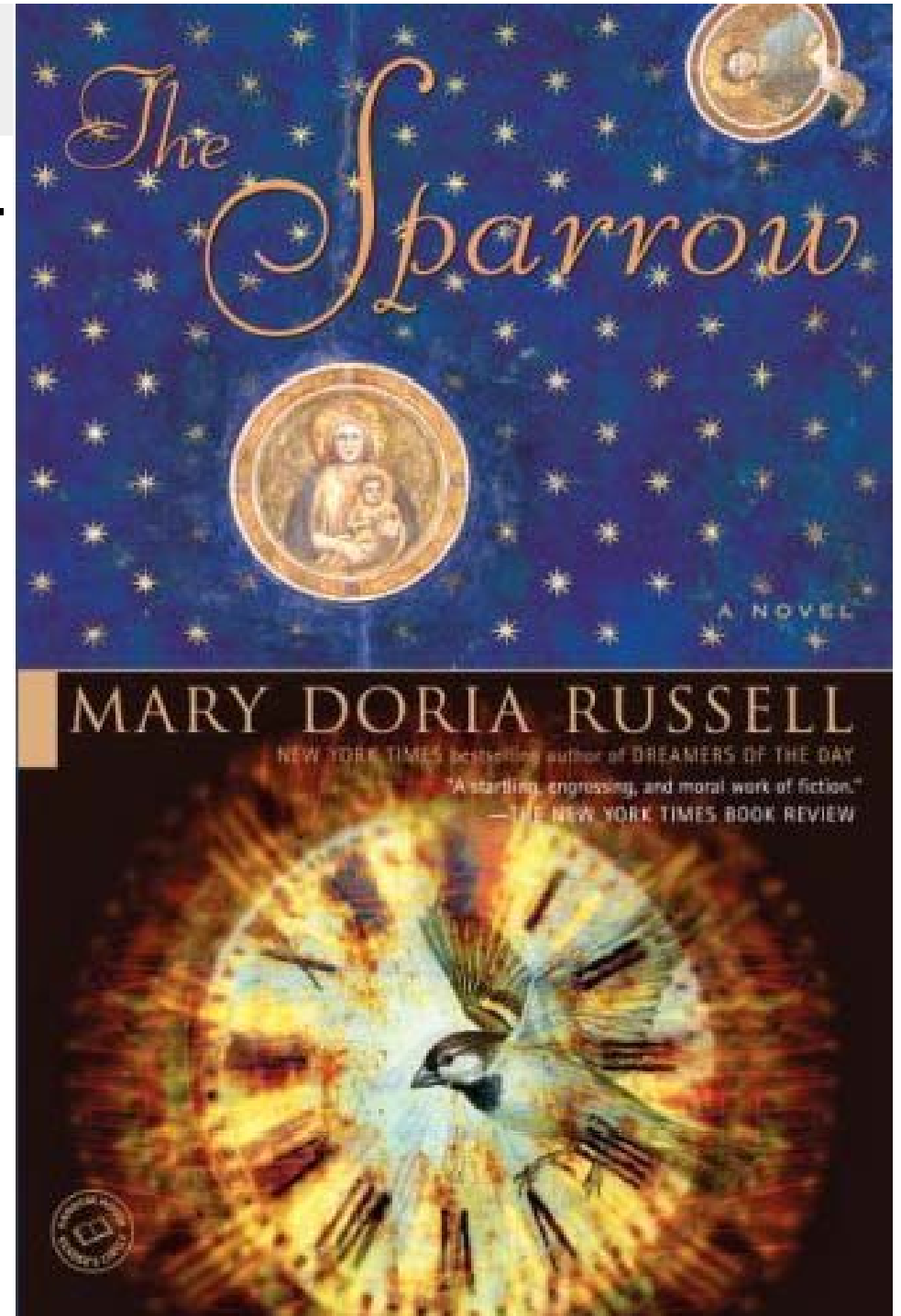
**Academic, publishing anthropologist.  
Converted from Catholic to Jew.  
First fiction book (1997).  
Wrote to resolve personal questions.**

**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.**



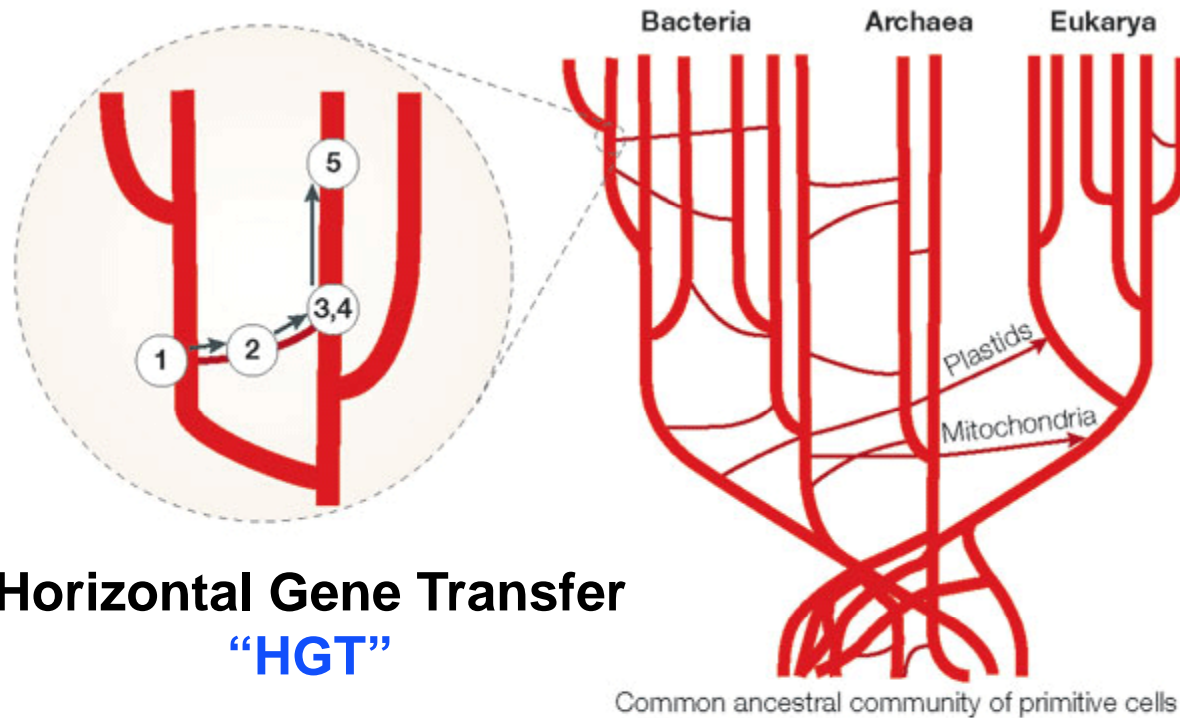
Woese, Carl. 2000. Interpreting the universal phylogenetic tree. PNAS. 97(15):8392-6. [www.ncbi.nlm.nih.gov/pmc/articles/PMC26958/pdf/pq008392.pdf](http://www.ncbi.nlm.nih.gov/pmc/articles/PMC26958/pdf/pq008392.pdf)

***“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.”***



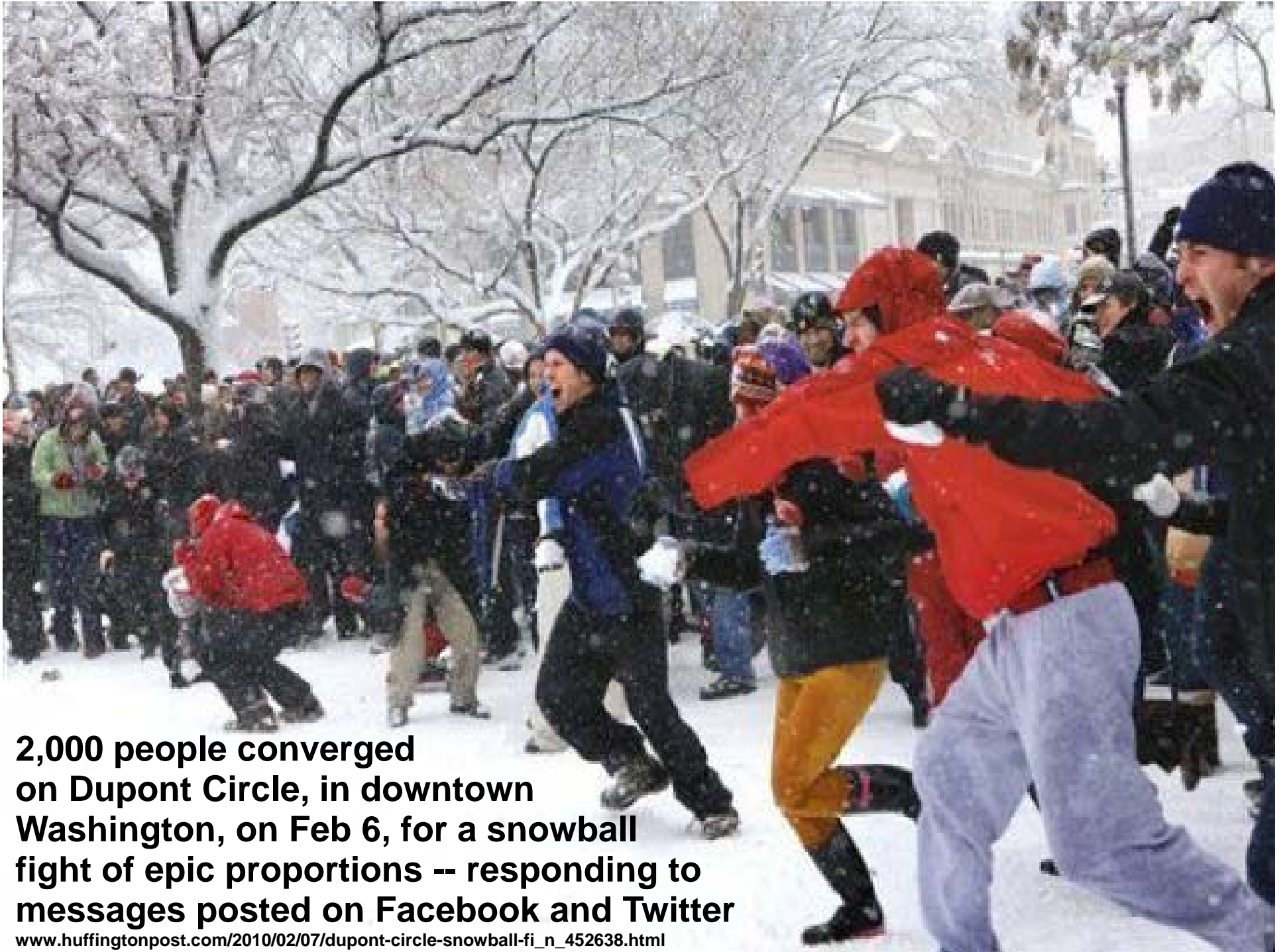
**Horizontal Gene Transfer**  
**“HGT”**

Common ancestral community of primitive cells

Copyright © 2005 Nature Publishing Group

**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).



**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](http://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](http://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

March 24, 2010, [www.nytimes.com/2010/03/25/us/25mobs.html?hp](http://www.nytimes.com/2010/03/25/us/25mobs.html?hp)

# March 20: Philadelphia Text-Message Flash Mob Horizontal Meme Transfer (HMT)



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

A container is parachuted to a ship being held by Somali pirates on Jan. 9. It's believed the container held ransom money for the ship and its crew — the usual way pirates collect "pay" for their "work" in the piracy business model.



## The Business Plan Of Pirates Inc.

[www.npr.org/templates/story/story.php?storyId=103657301](http://www.npr.org/templates/story/story.php?storyId=103657301)  
Chana Joffe-Walt, NPR – All Things Considered, April 30, 2009

**A piracy operation begins, as with any other start-up business, with venture capital.**

**J. Peter Pham at James Madison University says piracy financiers are usually ethnic Somali businessmen who live outside the country and who typically call a relative in Somalia and**

**suggest they launch a piracy business. The investor will offer \$250,000 or more in seed money, while the relative goes shopping.**

**"You'll need some speedboats; you'll need some weapons; you also need some intelligence because you can't troll the Indian Ocean, a million square miles, looking for merchant vessels," says Pham, adding that the pirates also need food for the voyage — "a caterer."**

**The pirates must choose their target carefully. "Does it have any value? Who is the crew? Do they have any security onboard? Who owns the ship? All of those things have to be factored. This is a business decision, to seize a ship. Westerners command a lot more money than poor Filipinos, whose country and families don't have the money to ransom them," Pham says.**

**Time sheets clocking pirates in and out were found after one calmly negotiated piracy ended. From this and other ransom situations, here's a typical accounting for a piracy operation: About 20 percent goes to pay off officials who look the other way. About 50 percent is for expenses and payroll. The leader of an attack makes \$10,000 to \$20,000 (the average Somali family lives on \$500 a year). The initial investor — who put in \$250,000 of seed capital — gets 30 percent, sometimes up to \$500,000.**



The austere bedroom of a Chinese hacker.  
Legions of hackers are pilfering information from individuals, corporations and government.

## Hacking for Fun & Profit in China's Underworld

01Feb2010, David Barboza, New York Times,  
[www.nytimes.com/2010/02/02/business/global/02hacker.html?hp](http://www.nytimes.com/2010/02/02/business/global/02hacker.html?hp)

Majia, a soft-spoken college graduate in his early 20s, is a cyberthief.

China has legions of hackers just like Majia, and they are behind an escalating number of global attacks to steal credit card numbers, commit corporate espionage and even wage online warfare on other nations.

In addition to independent criminals like Majia, there are so-called patriotic hackers who focus their attacks on political targets. Then there are the intelligence-oriented hackers inside the People's Liberation Army, as well as more shadowy groups that are believed to work with the state government.

In China — as in parts of Eastern Europe and Russia — **computer hacking has become a national sport, and a lucrative one. There are hacker conferences, hacker training academies and magazines** with names like Hacker X Files and Hacker Defense, which offer tips on how to break into computers or build a Trojan horse, step by step.

**Many Chinese hackers interviewed over the last few weeks describe a loosely defined community of computer devotees working independently, but also selling services to corporations and even the military.**



# Password Hackers Do Big Business With Ex-Lovers

Washington Post , Tom Jackman, 07Sep09: "When Elaine Cioni found out that her married boyfriend had other girlfriends, she became obsessed, federal prosecutors say. So she turned to YourHackerz.com.

And for only \$100, YourHackerz.com provided Cioni, then living in Northern Virginia, with the password to her boyfriend's AOL e-mail account, court records show. For another \$100, she got her boyfriend's wife's e-mail password. And then the passwords of at least one other girlfriend and the boyfriend's two children. None had any clue what Cioni was doing, they would later testify.

Cioni, however, went further and began making harassing phone calls to her boyfriend and his family, using a "spoofing" service to disguise her voice as a man's. This attracted the attention of federal authorities, who prosecuted Cioni, 53, in Alexandria last year for unauthorized access to computers, among other crimes. She was convicted and is serving a 15-month sentence.

But such services as YourHackerz.com are still active and plentiful, with clever names like "piratecrackers.com" and "hackmail.net." They boast of having little trouble hacking into such Web-based e-mail systems as AOL, Yahoo, Gmail, Facebook and Hotmail, and they advertise openly.

...

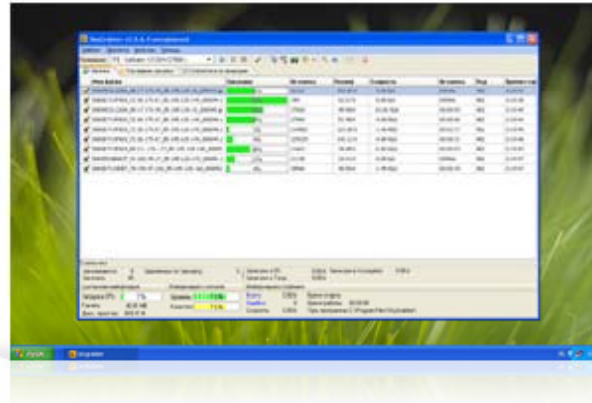
At SlickHackers.com, they boast, "We are professionals interested in helping serious people for whom an email password would mean saving their marriage, knowing the truth, preventing a fraud, protecting their family/job/interests only when conventional ways and normal procedures do not work."



# SkyGrabber

satellite internet downloader

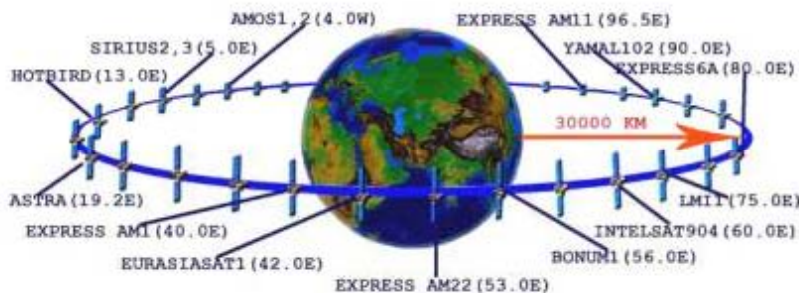
SkyGrabber is offline satellite internet downloader. It intercepts satellite data ( movie, music, pictures ) that downloading by other users and saves information in your hard disk. So, you'll get new movie, best music and funny pictures for free.



You don't have to keep an online internet connection. Just customize your satellite dish to selected satellite provider and start grabbing. SkyGrabber has simple and attractive GUI, powerful filter system and flexible settings. If you want to have newest software for free, SkyGrabber is your choice.

## How it all works?

There are different types of Internet connection, such as Dial-Up, ADSL, Leased Line, etc. Satellite internet is a kind of Internet connection and is used mainly in remote areas or in areas where Internet access is problematic because of its lack, or slow speed of the high cost of local Internet connections.



Ads by Google

[HughesNet vs Other Guys](#)  
Compare Satellite Internet Providers and You Decide!  
[elitesat.com/\\_HughesNe](http://elitesat.com/_HughesNe)



Ads by Google

- [Free Satellite TV](#)
- [WiFi Antenna Booster](#)
- [Windom Antenna](#)
- [Satellite Radio](#)
- [Digital Satellite](#)

Google Ads



Ads by Google

[Wild Blue • \\$49 Special](#)  
Get WildBlue High Speed From \$49.95 Offer Ends Soon, Order Today!  
[www.WildBlueDeals.com](http://www.WildBlueDeals.com)



\$26 software advertised blatantly as application for stealing satellite downloads:

movies, software, others email

...and even unencrypted live military feeds from UAV drones.

Integrated in the global economy...

Ads by Google

# Decentralized IED Marketplace in Iraq

[http://globalguerrillas.typepad.com/globalguerrillas/2005/08/the\\_ied\\_marketp.html](http://globalguerrillas.typepad.com/globalguerrillas/2005/08/the_ied_marketp.html)

Number of IED events a day: 40 (exploded or disarmed)

**Decentralized Structure:** *Vast numbers of small, adaptive insurgent cells operate independently without central guidance.*

**Commercial Connections:** *Small, highly skilled IED cells often operate as a package and hire themselves out to the more well-known insurgent groups. They advertise their skills on the Internet and are contracted on a per-job basis.*

**Target Selection:** *with PR through media exposure -- which also acts as a means of stigmergy between groups.*

**Training:** *They videotape IED attacks, study them to prepare for future attacks, use as motivational tools for new recruits, and to advertise technical proficiency.*

**Business Process – Financier:** *At the top of the IED cell is the planner or financier, a "money man" who is most often a well educated and intelligent former government official or military officer.*

**Business Process – Bomb Maker:** *Bomb-making skills proliferate rapidly among IED cells in Iraq via the Internet, used by insurgents to share skills.*

**Business Process – Emplacer:** *The emplacer's primary motivation is money. He is a foot soldier, is often paid as little as \$50, and told to place an IED in a specific location at a specific time.*

**Business Process – Triggerman:** *primary motivation is money. Sometimes these operatives will hire themselves out as a package, changing affiliations for money.*

**Business Process – Suicide Car Bombers:** *Car bombs are assembled in a factory assembly line-like process. As the vehicle is driven north to Baghdad additional components are added. Decentralization makes finding bomb factories hard.*

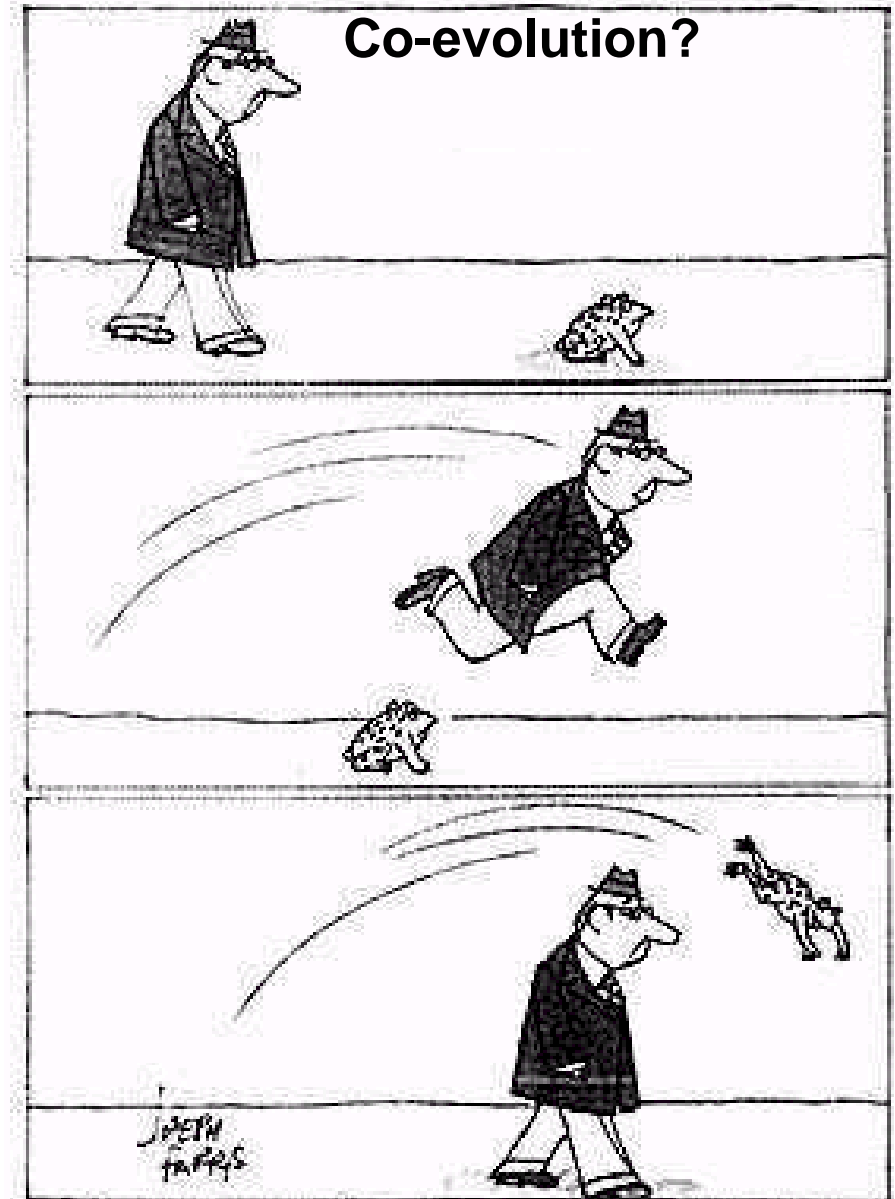
# HMT = Adversarial Advantage (Horizontal Meme Transfer)

## Architecture:

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

## Behavior:

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



# HMT = Adversarial Advantage

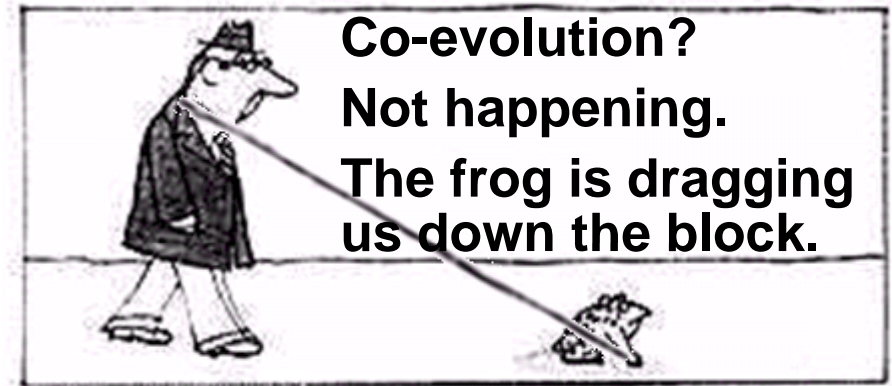
(Horizontal Meme Transfer)

## 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



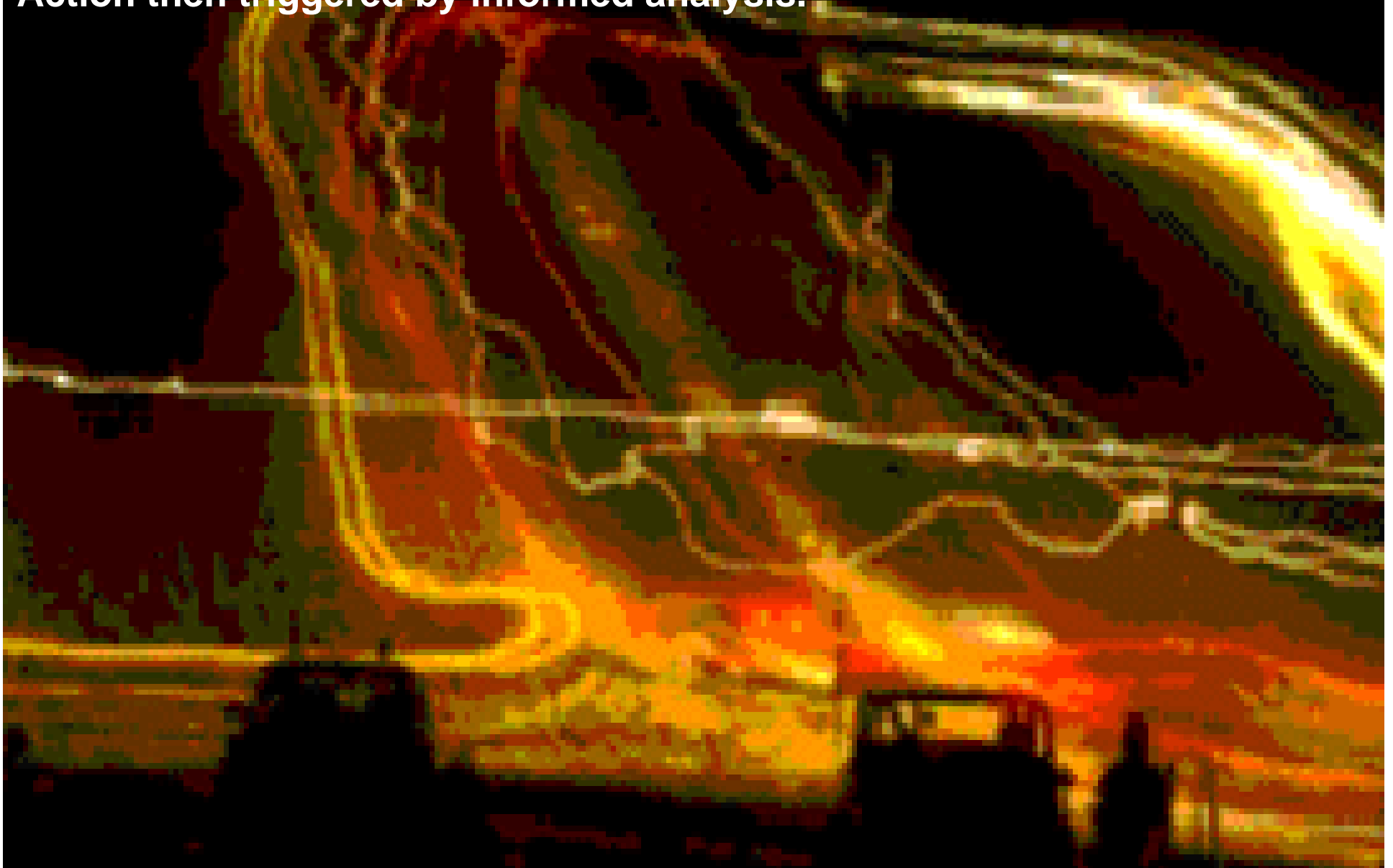
**Agile system security, as a minimum, must mirror the agile characteristics exhibited by the system attack community:**

- [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.



# Incident-Response Flash Communities

Independent “agents” come together as a system of systems when some catalyzing event occurs that either threatens them individually and collectively, or otherwise causes them to work collectively against some perceived evil.

Alex Lightman and Rachel Coleman. 2009. [Search and Destroy Engines](#). h+ Magazine, June 2, [www.hplusmagazine.com/articles/politics/search-and-destroy-engines](http://www.hplusmagazine.com/articles/politics/search-and-destroy-engines)

Argonne National Laboratory. 2009. [Argonne develops program for cyber security “Neighborhood Watch”](#). Argonne National Laboratory Newsroom. July 16. [www.anl.gov/Media\\_Center/News/2009/news090716.html](http://www.anl.gov/Media_Center/News/2009/news090716.html)

Khurana, Himanshu, Jim Basney, Mehedi Bakht, Mike Freemon, VonWelch, Randy Butler. 2009. [Palantir: A Framework for Collaborative Incident Response and Investigation](#). In Proceedings Symposium on Identity and Trust on the Internet (IDTrust), Gaithersburg, MD, April 14-16. <http://netfiles.uiuc.edu/hkhurana/www/IDTrust20091.pdf>

Internet Storm Center .... and many more



# Armchair deputies patrol US-Mexico border

<http://news.bbc.co.uk/2/hi/americas/8412603.stm>

**Crowd Sourcing**  
– one of many examples

When John Spears gets home from his sales job in New York, he sits down at his computer with a bottle of beer and starts patrolling the US border. There are live feeds 24/7 from 21 surveillance cameras placed along the border.

He is one of many who are volunteering to patrol the 1250-mile long (2000 km) stretch between Texas and Mexico via the web.

Since the site went live in November 2008 more than 130,000 people have registered to become “virtual deputies”, located as far as Australia, Mexico, Colombia, Israel, New Zealand and the UK.

**BLUESERVO.NET**

# Maslow's Hierarchy of Needs

## Maslow's Hierarchy of Needs



Art: [www.abraham-maslow.com/m\\_motivation/Hierarchy\\_of\\_Needs.asp](http://www.abraham-maslow.com/m_motivation/Hierarchy_of_Needs.asp)

# Maslow's Hierarchy of Needs

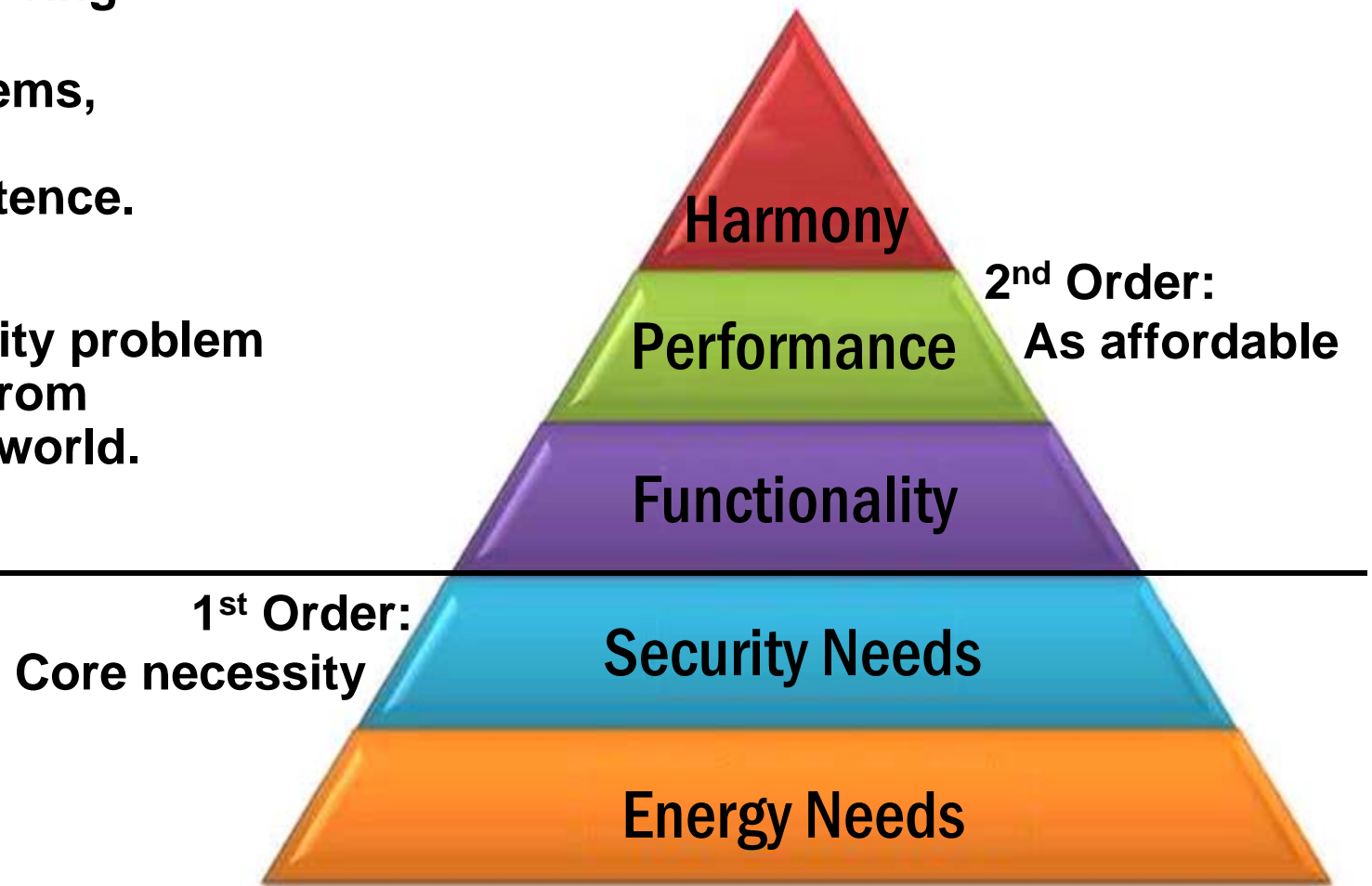
(for systems that would live one more day)

**Its Not About Cyber Security**  
(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



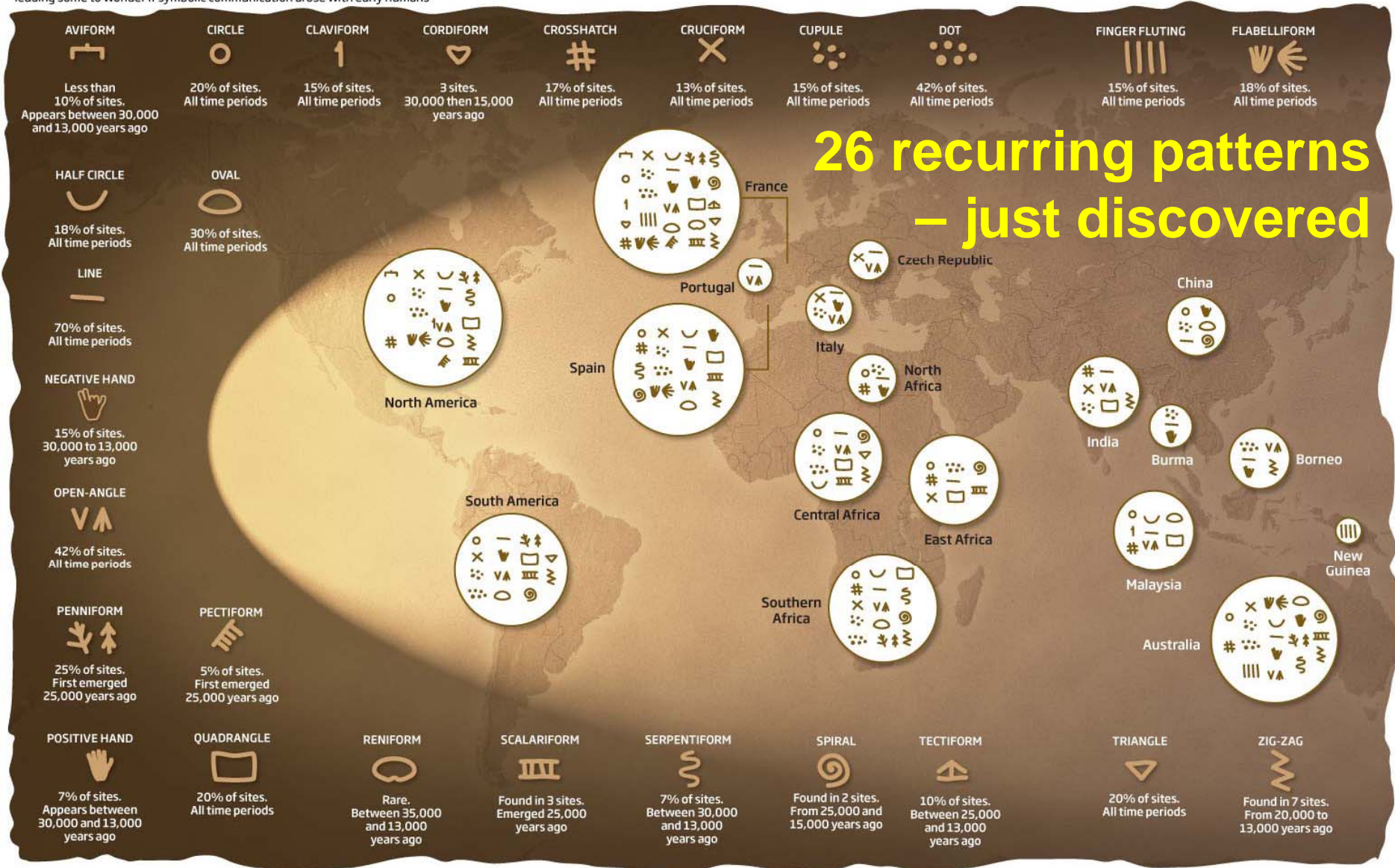
# Cave signs from 146 sites in France, covering 35,000 to 10,000 years ago. What emerged was startling: 26 signs, all drawn in the same style, appeared again and again at numerous sites.

## Stone Age jottings

French caves are known for their prehistoric rock art. But also marked on the walls around the paintings are 26 symbols that have appeared again and again at French sites across 25,000 years of prehistory. Early signs suggest that many of these symbols crop up in other parts of the world too, leading some to wonder if symbolic communication arose with early humans

©NewScientist

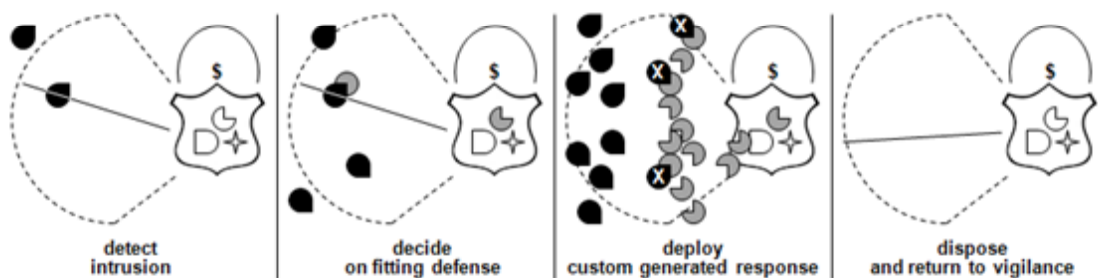
17Feb2010, New Scientist Magazine issue 2748. Also see: <http://communications.uvic.ca/releases/makepdf.php?type=tip&date=22022010>



SOURCE: GENEVIEVE VON PETZINGER, ANDRE LEROU-COURHON, DAVID LEWIS, WILLIAMS, MARILE FRANKLIN

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

**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.

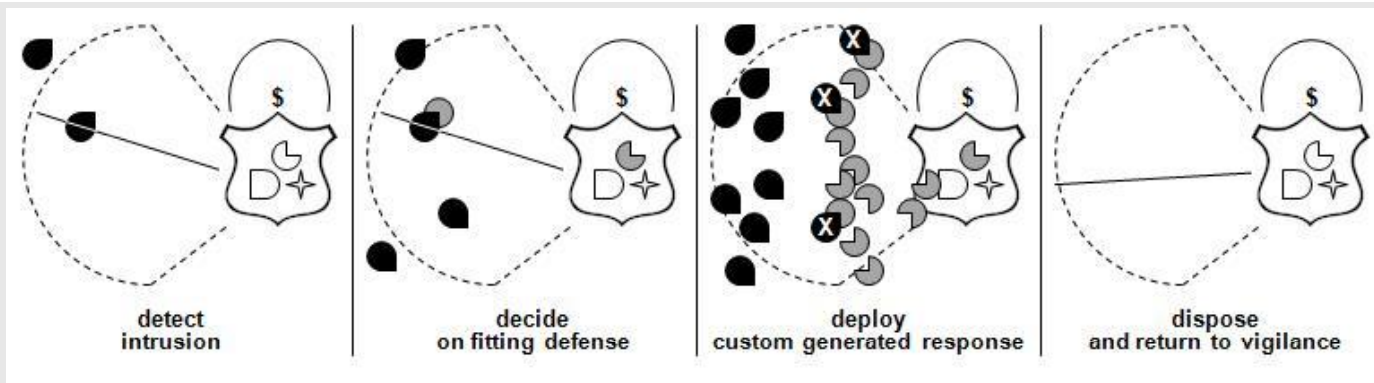
<b>Name:</b> Dynamic Phalanx Defense
<b>Context:</b> a stationary or mobile asset subject to unpredictable swarm attacks.
<b>Problem:</b> Attackers can come in many and unpredictable forms, and in virtually unbounded quantities, with no advance warning. For instance, A DDoS attack on an Internet service node may be of many different types; an attack on a naval asset may be surface, undersea or air in many different varieties.
<b>Forces:</b> Resilience of service vs. cost of service. Comprehensive counter capability and capacity vs cost and disharmony of a broad standing counter force.
<b>Solution:</b> 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 style="text-align: center;">Aggressive shield waxes and wanes measure-for-measure in real time</p>
<b>Example:</b> 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).
<b>Example:</b> 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).
<b>Example:</b> Just-in-time drone swarms – Load disposable drones with modular sensor and weapon choices, and deploy quantities as needed. See SWARM, IITSA discussion in (Hambling 2006).
<b>Example:</b> Plant chemical defense – Insect saliva triggers selective toxic gene expression and gas emissions that call in selective insect predators.,
<b>Agility:</b> 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]
<b>References:</b> (see reference section, only URL shown here, all accessed 30Nov09) <ul style="list-style-type: none"> <li>• (Dixon et al. 2008) <a href="http://www.cs.washington.edu/homes/ckd/phalanx.pdf">www.cs.washington.edu/homes/ckd/phalanx.pdf</a>.</li> <li>• (Edge et al. 2006) <a href="http://paper.ijcsns.org/07_book/200603/200603C08.pdf">http://paper.ijcsns.org/07_book/200603/200603C08.pdf</a></li> <li>• (Hambling 2006) <a href="http://defensetech.org/2006/04/10/drone-swarm-for-maximum-harm/">http://defensetech.org/2006/04/10/drone-swarm-for-maximum-harm/</a></li> <li>• (Mahimkar et al. 2007) <a href="http://www.cs.utexas.edu/~yzhang/papers/dfence-nsdi07.pdf">www.cs.utexas.edu/~yzhang/papers/dfence-nsdi07.pdf</a></li> <li>• (Wilkinson 2001) <a href="http://pubs.acs.org/cen/critter/plantsbugs.html">http://pubs.acs.org/cen/critter/plantsbugs.html</a></li> <li>• (Zhang et al. 2008) <a href="http://www.computer.org/portal/web/csdi/doi/10.1109/ICNC.2008.782">www.computer.org/portal/web/csdi/doi/10.1109/ICNC.2008.782</a></li> </ul>

# Dynamic Phalanx Defense<sup>1/3</sup>

<b>Name:</b>	<b>Dynamic Phalanx Defense</b>
<b>Context:</b>	a stationary or mobile asset subject to unpredictable swarm attacks.
<b>Problem:</b>	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.
<b>Forces:</b>	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.

**Graphic:**

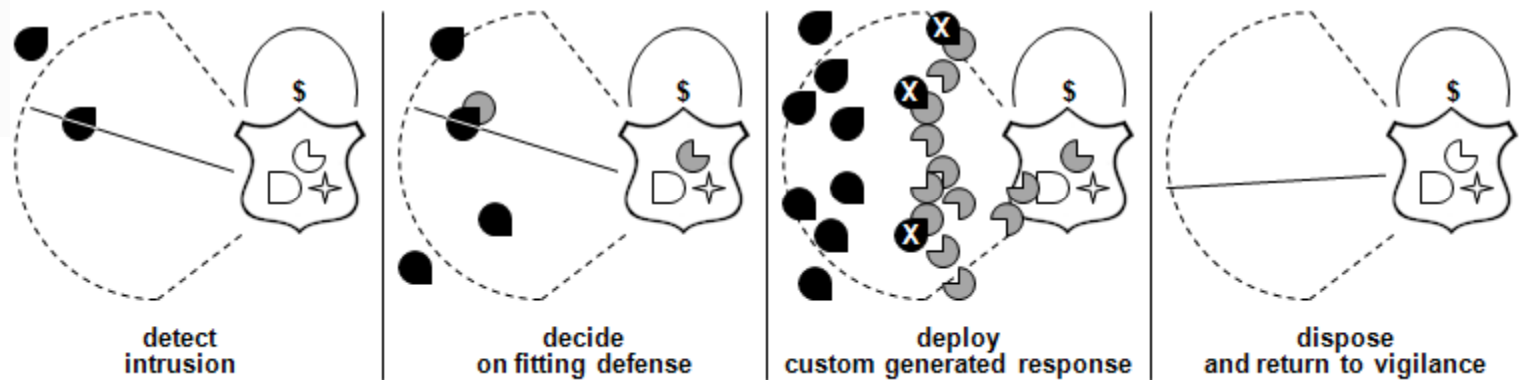


**Agility:** Self organization grows and shrinks a counter swarm in measured response to an attack swarm. Adaptability selects appropriate counter-swarm agents from modular resources. Resilience is exhibited with expendable and replicable counter agents, and in continued operation of the protected asset, 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]



<p><b>Examples:</b></p>	<p><b>Botnet denial of service defense</b> – 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.  <a href="#">Phalanx: Withstanding Multimillion-Node Botnets</a> (<u>Dixon et al. 2008</u>)  <a href="#">dFence: Transparent Network-based Denial of Service Mitigation</a> (<u>Mahimkar et al. 2007</u>)</p>
	<p><b>Just-in-time defensive drone swarms</b> – Sense and respond automatically to launch drone swarms against ambushes and flash threats to warfighting assets.  <a href="#">Drone Swarm for Maximum Harm</a> (<u>Hambling 2006</u>)</p>
	<p><b>Artificial immune system</b> – detection, selection, cloning and retirement applied to mobile network intrusion detection and repulsion.  <a href="#">Multi-objective Mobile Network Anomaly Intrusion</a> (<u>Edge et al. 2006</u>)  <a href="#">Network Intrusion Active Defense Model Based on Artificial Immune System</a> (<u>Zhang et al. 2008</u>) .</p>
	<p><b>Plant chemical defense</b> – 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.  <a href="#">Plants to Bugs: Buzz Off!</a> (<u>Wilkinson 2001</u>)</p>

## 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).**

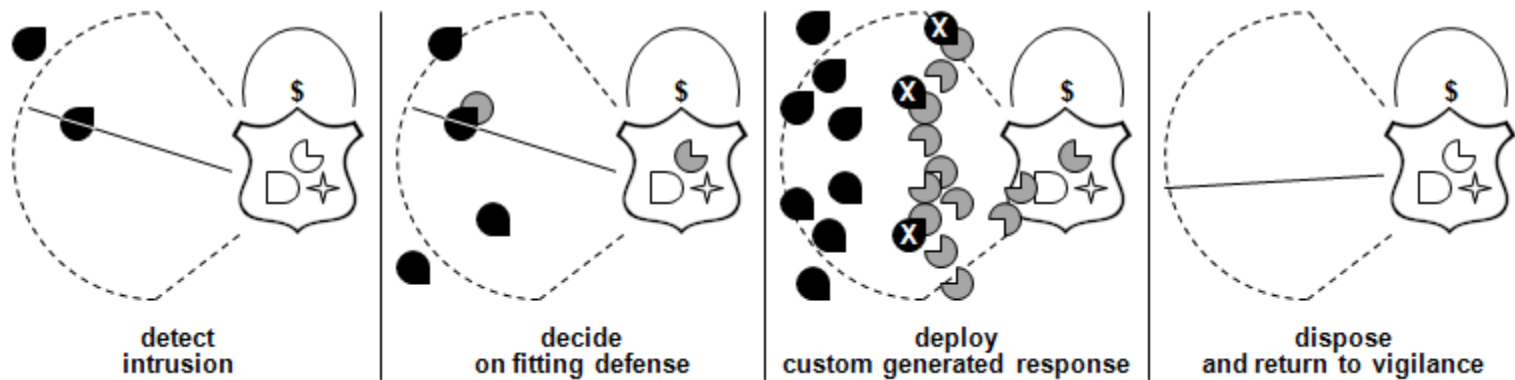
**Example: Just-in-time drone swarms – Load disposable drones with modular sensor and weapon choices, and deploy quantities as needed. See SWARM, JITSA discussion in (Hambling 2006).**

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

**Mostly systemically self-organized above – human directed examples include:**

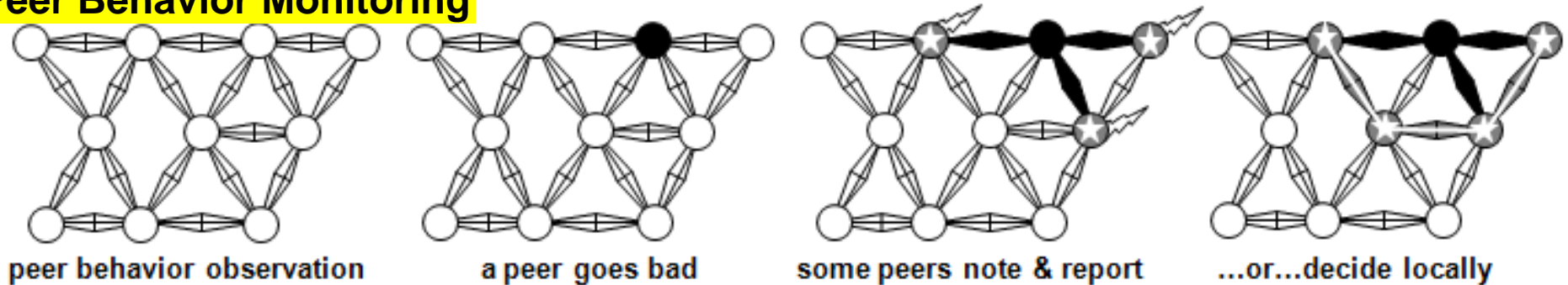
- NATO
- Internet Storm Center
- Fire department mutual aid
- Incident response coalitions (Khurana 2009)

## Dynamic Phalanx Defense



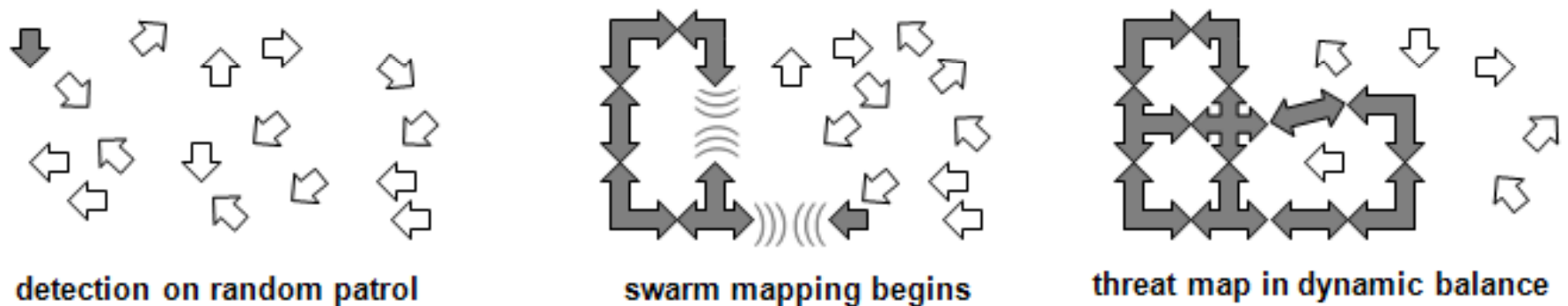
Aggressive shield waxes and wanes measure-for-measure in real time

## Peer Behavior Monitoring



Peers monitor for aberrant behavior and tattle or decide locally

## Swarming Threat Sensors

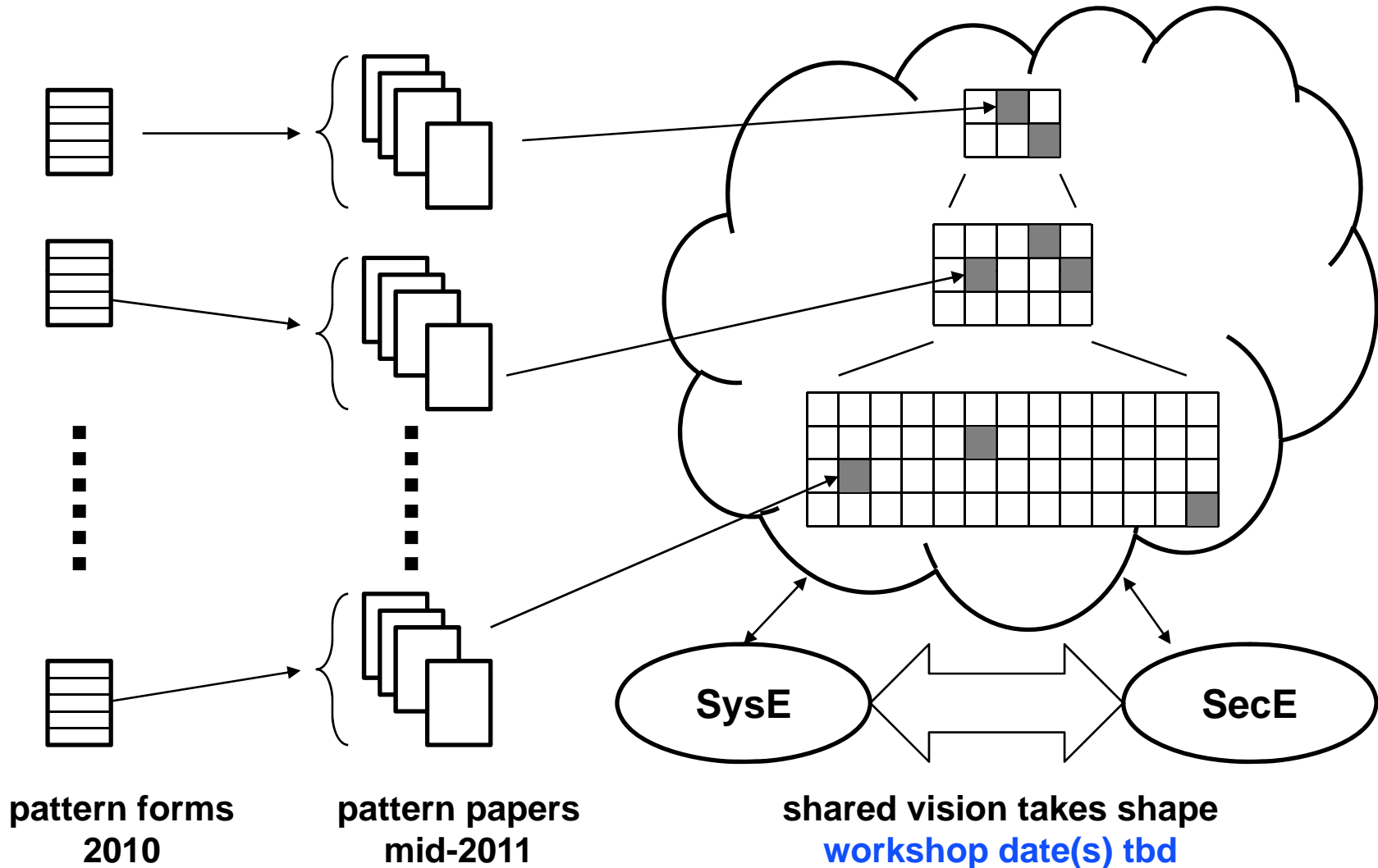


Swarm convergence seeks optimal sensor distribution to monitor detected threat

**P1: Formed Candidates**

**P2: Papers Detailing Single Patterns**

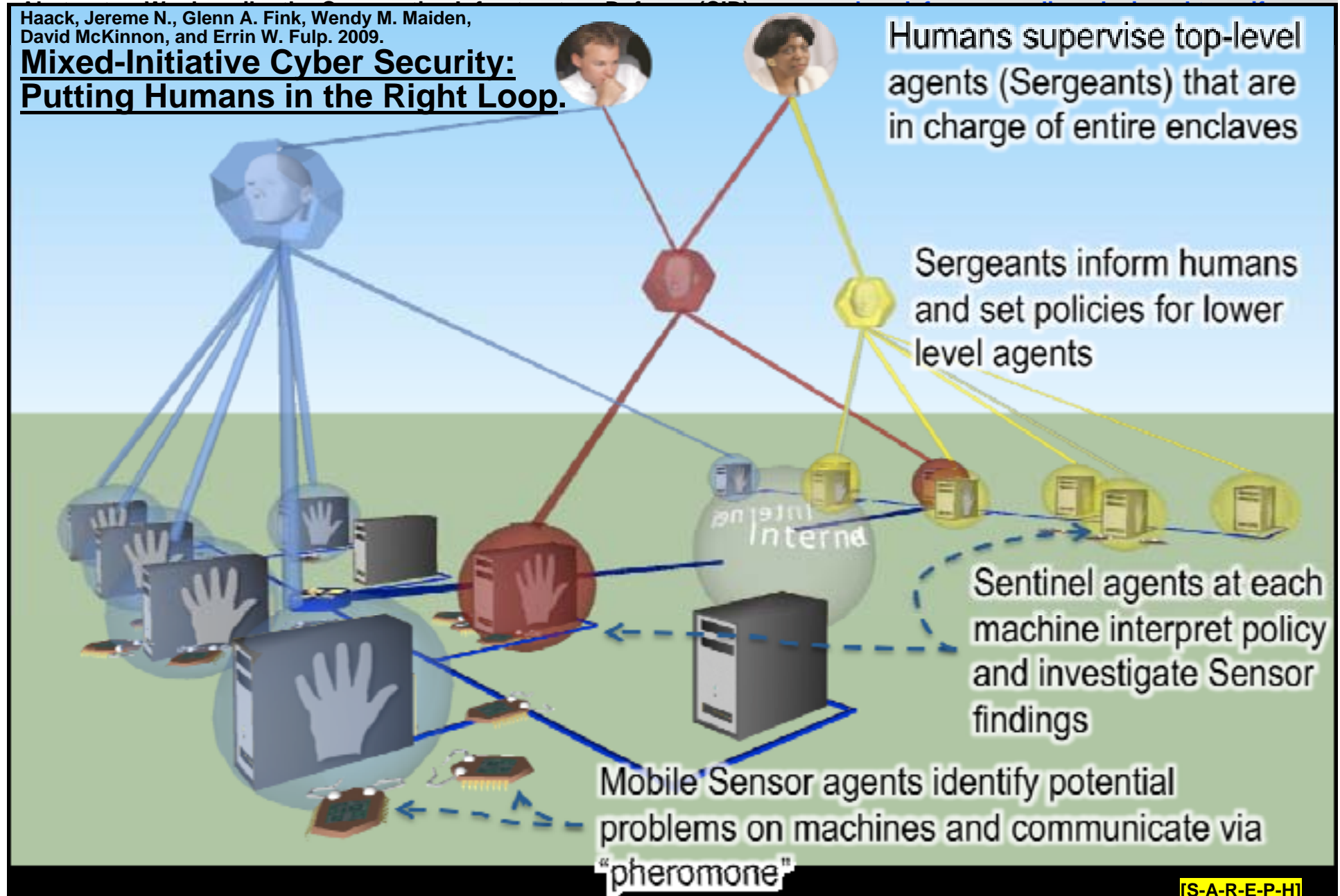
**P3: Instigating path-finder shape to the vague cloud**



# Candidate: Hierarchical Temporal memory (HTM = Cortical Sense Making Mechanism)

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.

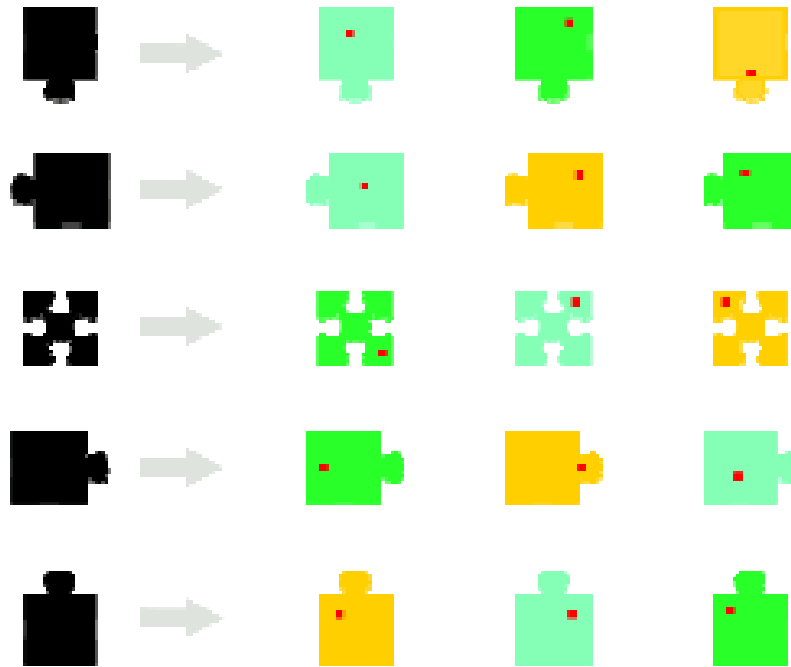


# Candidate: Component-Equivalent Diversity

Living systems adapt to cope with unknowable attacks

Genome

Alleles



- A component type is similar to a gene; component implementations are similar to alleles of a gene

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](http://portal.acm.org/beta/ft_gateway.cfm?id=1558643&type=pdf&CFID=82493696&CFTOKEN=93605741)

rick.dove@parshift.com, attributed copies permitted

S-A-R-P-H 30

# Candidate: Quorum Sensing

## Quorum sensing and social networking in the microbial world

5 Mar 2010, Hayley Birch, Issue 2750, [www.newscientist.com/article/mg20527501.300-bugging-bugs-learning-to-speak-microbe.html](http://www.newscientist.com/article/mg20527501.300-bugging-bugs-learning-to-speak-microbe.html)  
Atkinson, Steve and Paul Williams. 2009. J. Royal Society Interface 6, 959–978. <http://rsif.royalsocietypublishing.org/content/6/40/959.full>

Bacteria communicate using chemical signals, releasing and receiving signalling molecules in a process known as quorum sensing. In its simplest form, bacteria use quorum sensing to keep track of their neighbours. Some bioluminescent bacteria, for example, light up when their population exceeds a threshold size.

Our own cells exploit this same signalling system to monitor and cajole our personal population of microbes, just as they eavesdrop on and manipulate us. In other words, we don't passively host this bacterial colony, but actively engage it in conversation."

# Horizontal Meme Transfer (HMT)

A prime and necessary pattern for innovative evolution of security

The pattern that explains the research project:  
**find patterns across domains (a first?)**

**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.”**



## Multi-Range Weapons Testing System – UAST (highly stylized architectural concept diagram)

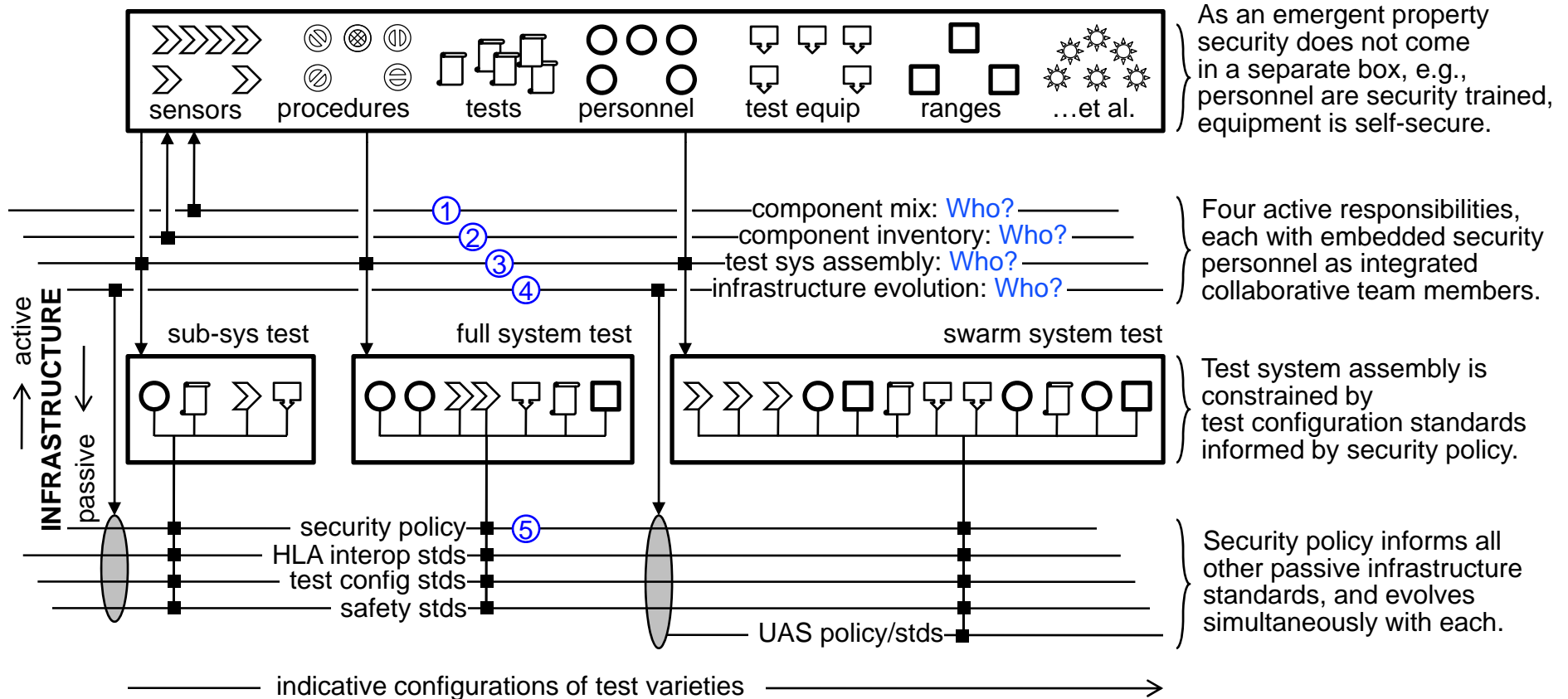
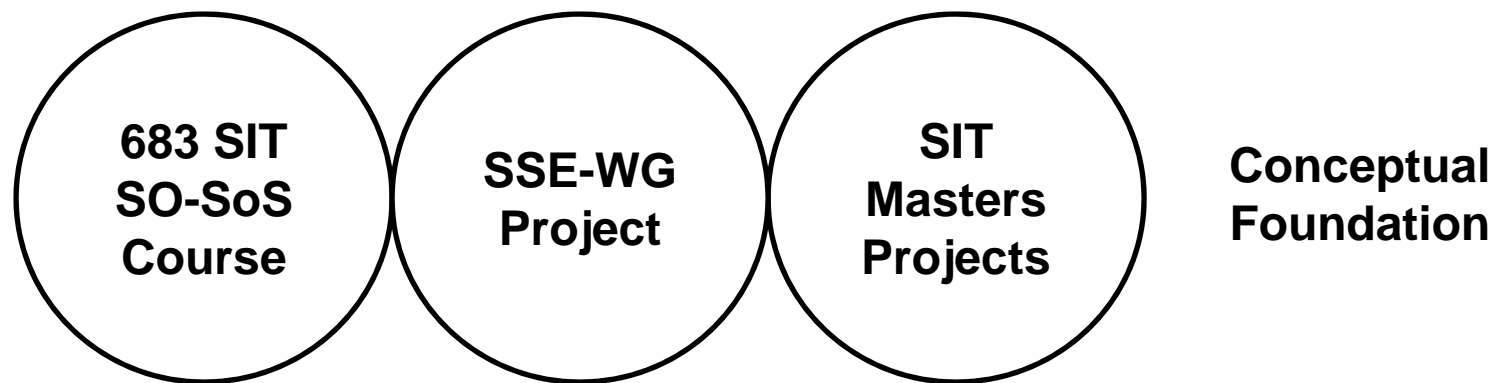


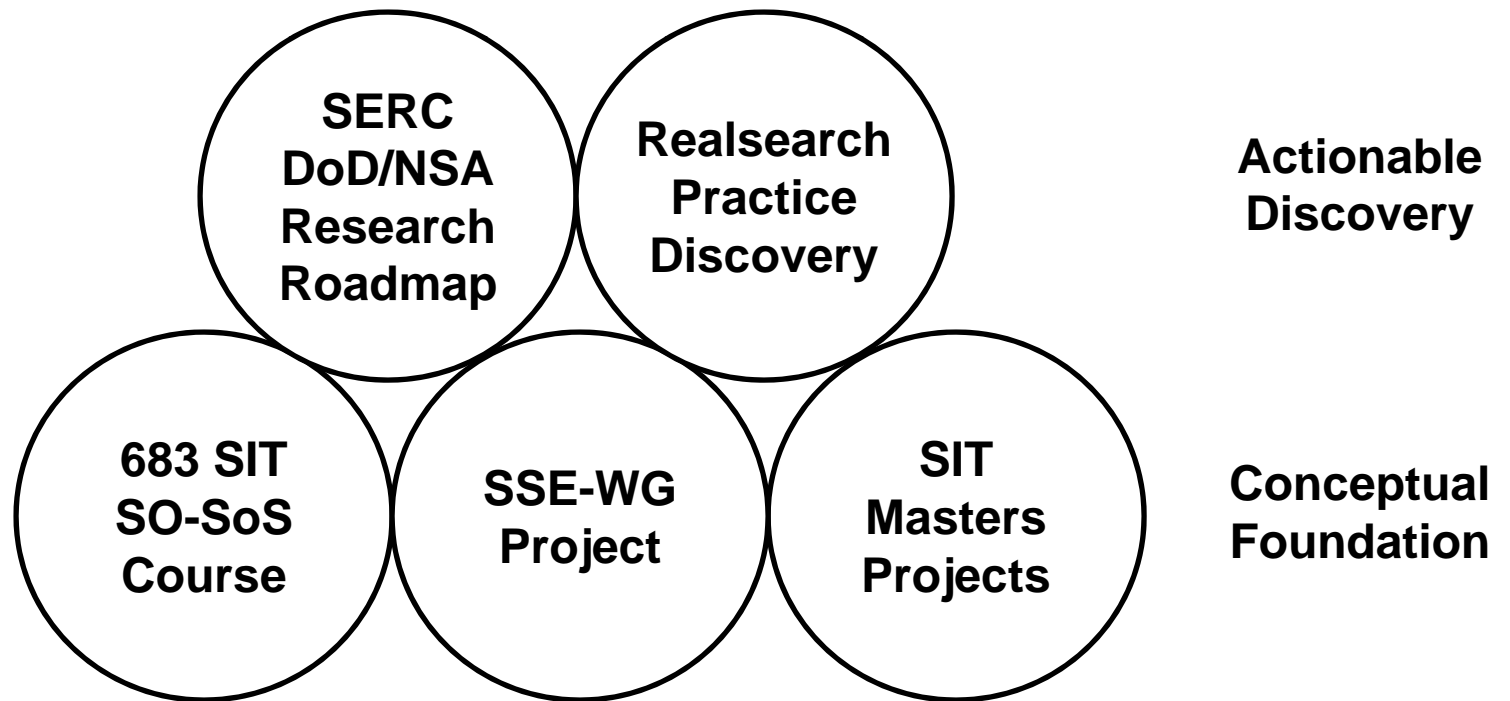
Figure 3. Security is embedded in architecture at points 1-5. Additionally, encapsulated components have internal security distrustful of other components in general, ideally a fractal image of this architecture.

# How Things are Stacking Up



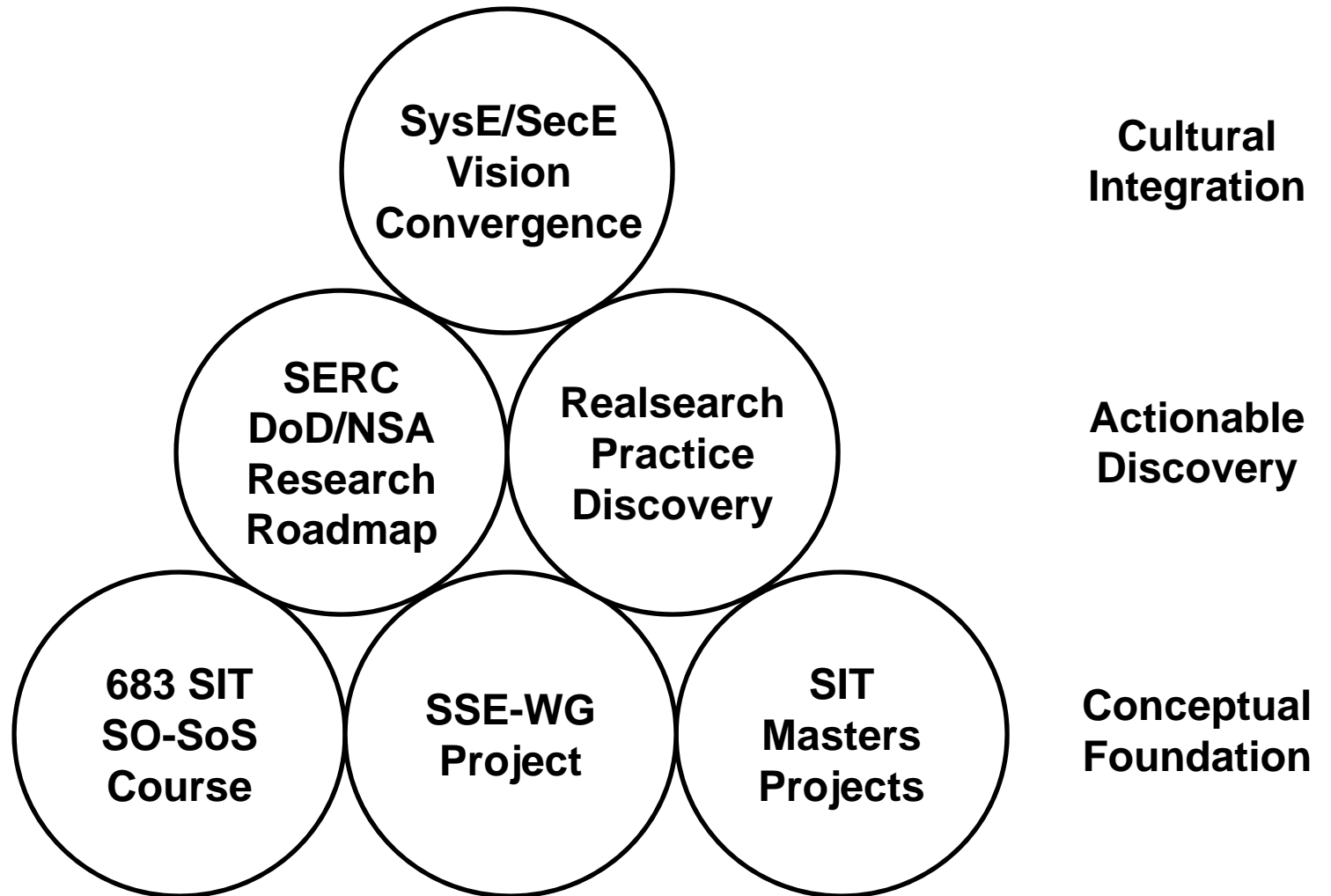
\*SIT: Stevens Institute of Technology

# How Things are Stacking Up



\*SIT: Stevens Institute of Technology

# How Things are Stacking Up



\*SIT: Stevens Institute of Technology

# Coming Soon: Realsearch

**Real people, working on Real problems, in Real time**

**Used for discovering agile systems principles in the '90s**

**5-10 3-day workshops – with specific pattern objective(s), e.g.:**  
**systemic/consortial, strategic/tactical,**  
**within/across domains, practitioners/decision-makers,**  
**...etc**

**Hosted at multiple places – with different interests**

**Host provides 5-10 participants**

**Travelers provide 5-10 participants**

**Tool (framework)-driven analysis and synthesis**

**Actionable results for participants**

**Findings are amalgamated and published as related-pattern collection**

## **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

**You can be in the vanguard of SO-SoS pattern discovery**

- suggested pattern concepts can be provided
- source reference material can be provided
- collaboration will be provided

- 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](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](http://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](http://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](http://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](http://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](http://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](http://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.