

SC2RAM: A Deployable Cognitive Model of a Cyber- Attacker

Van Parunak, Randy Jones
Soar Technology, Inc.
{van.parunak, rjones}@soartech.com



SOARTECH

Modeling human reasoning.
Enhancing human performance.



Persistent: Carried out over an extended period of time

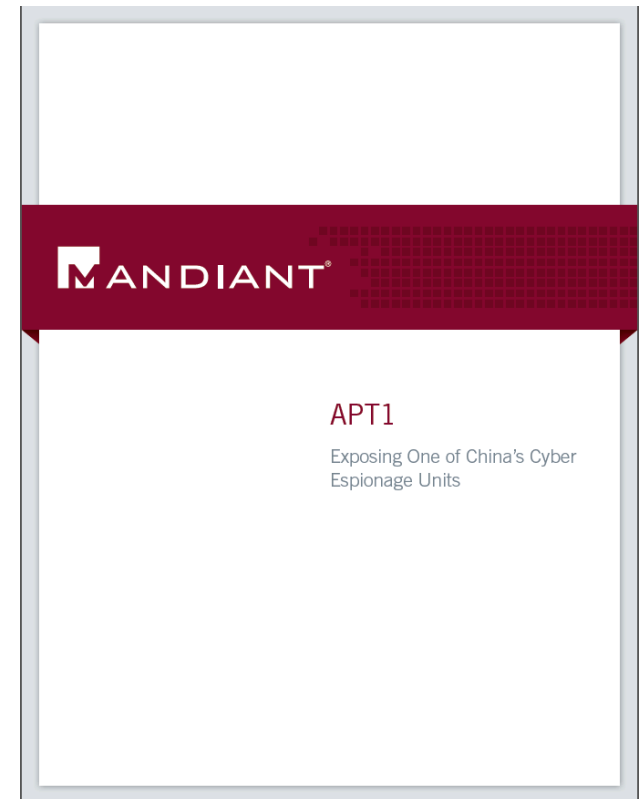
Advanced: Multiple different steps, strategically related (e.g., initial compromise, establish foothold, escalate privileges, internal reconnaissance, move laterally, maintain presence, complete mission)

Adaptive: Human cognitive behavior

- *Sense* defensive actions and respond
- *Learn* from experience
- *Innovate* new actions
- *Interact* with (human and computer) colleagues

Highly-skilled **human Red Teams** are needed to

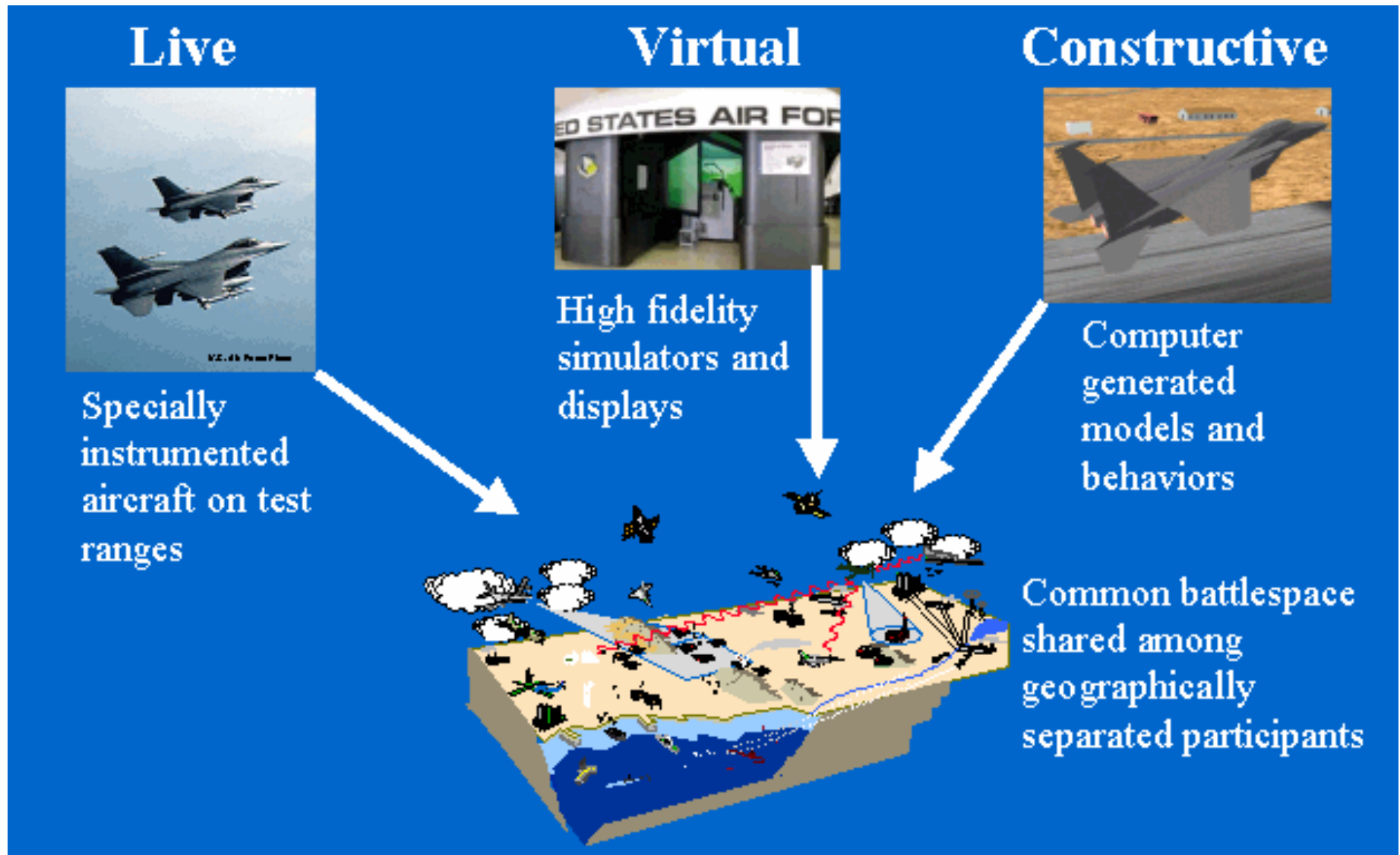
- *Train* system operators to deflect such threats
- *Configure and test* defensive systems
- *Wargame* the cyber-ecology to develop TTPs

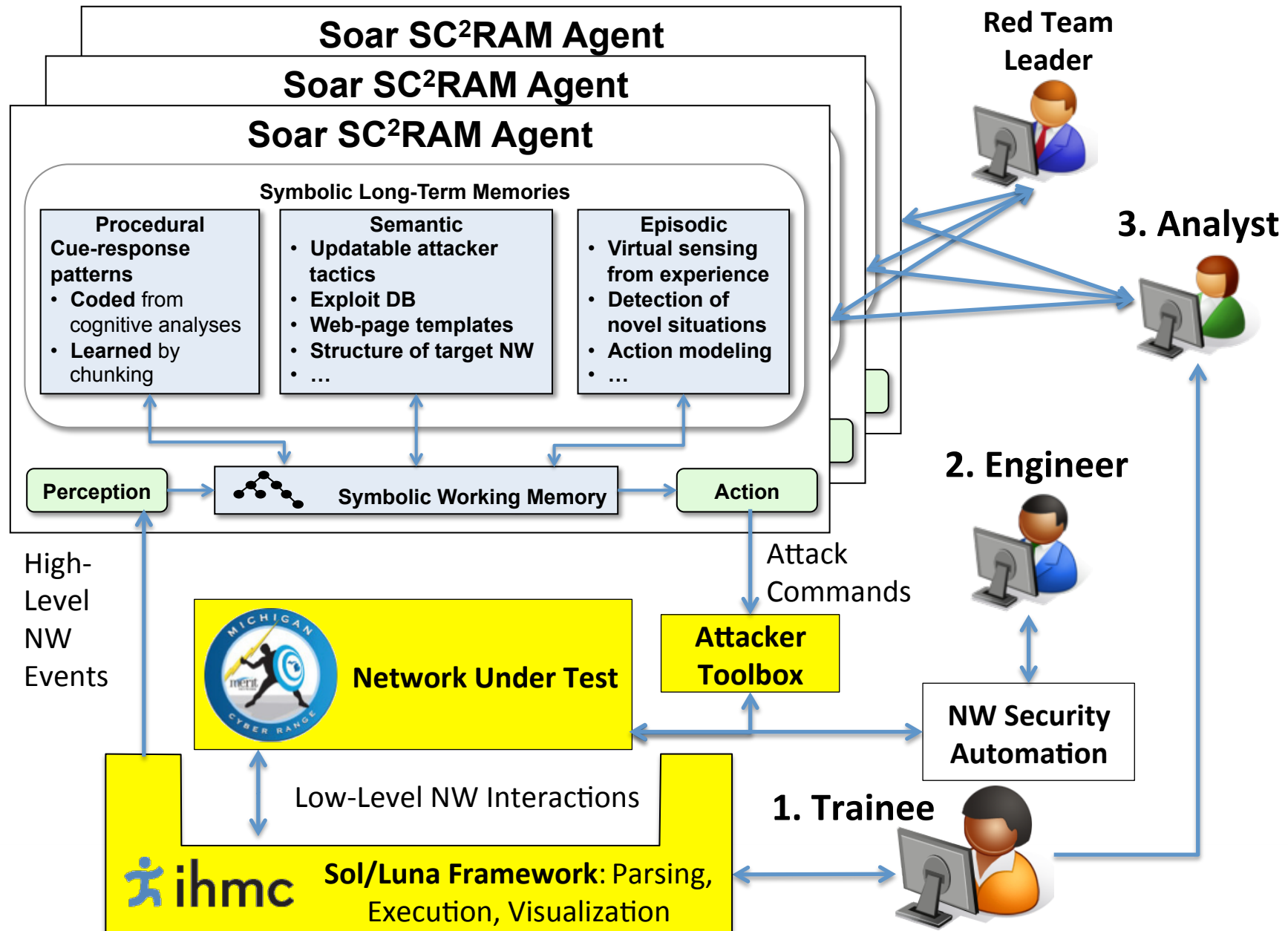


www.mandiant.com/apt1

→ **SC2RAM:** Simulated Cognitive Cyber Red-team Attacker Model

The TAC-AIR Soar Heritage in LVC Simulations

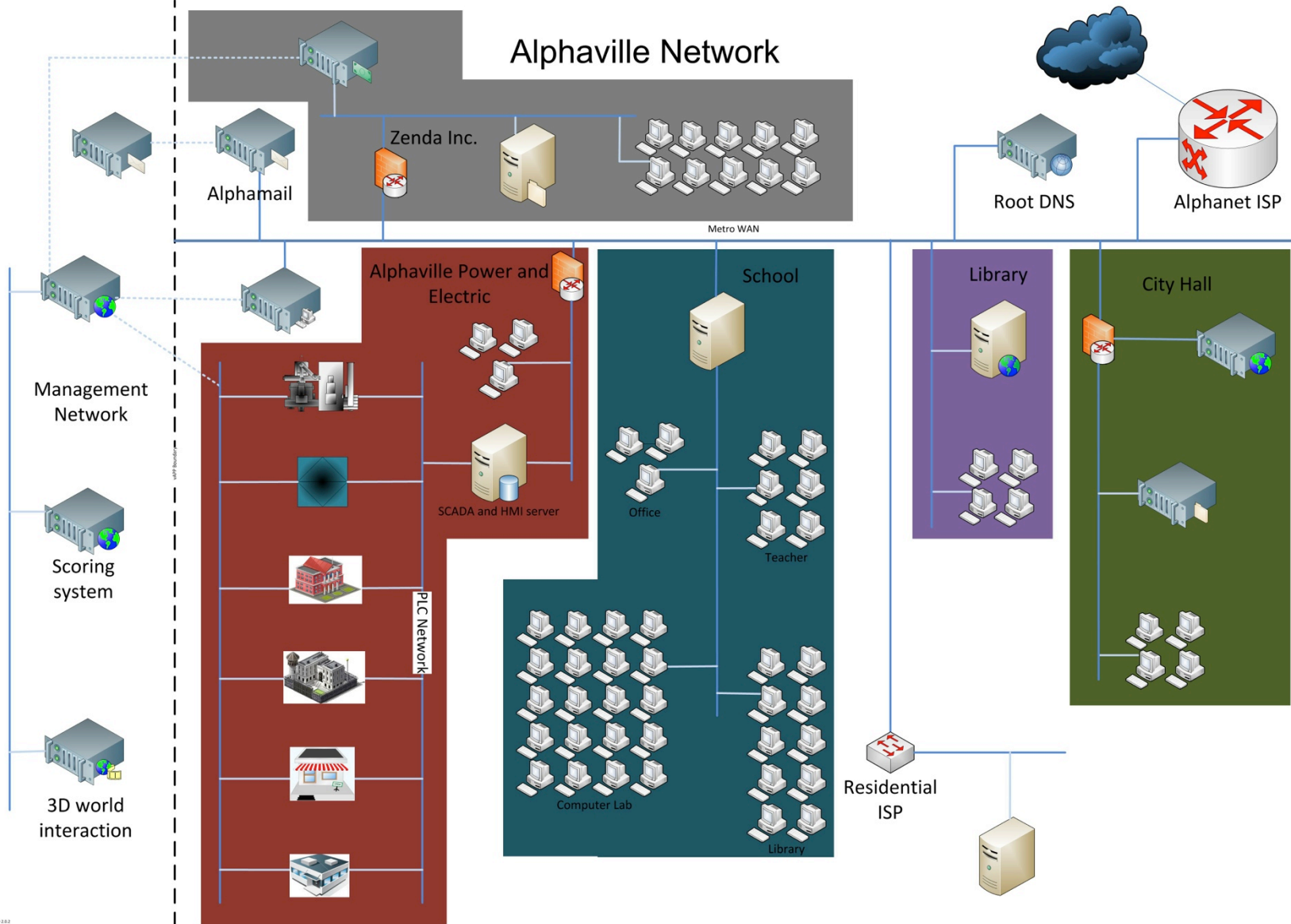






Alphaville

MICHIGAN CYBER RANGE

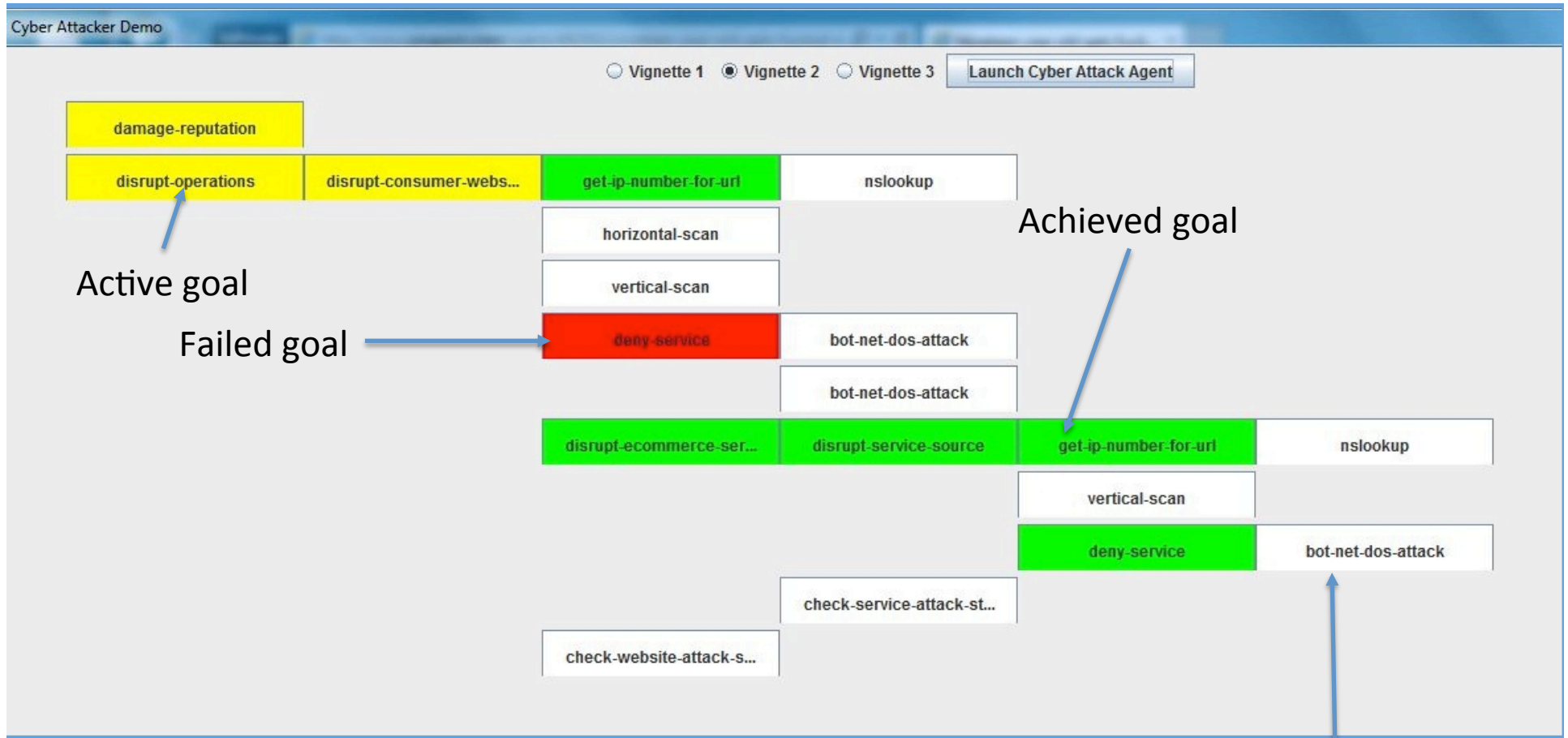


Demo: Three Vignettes

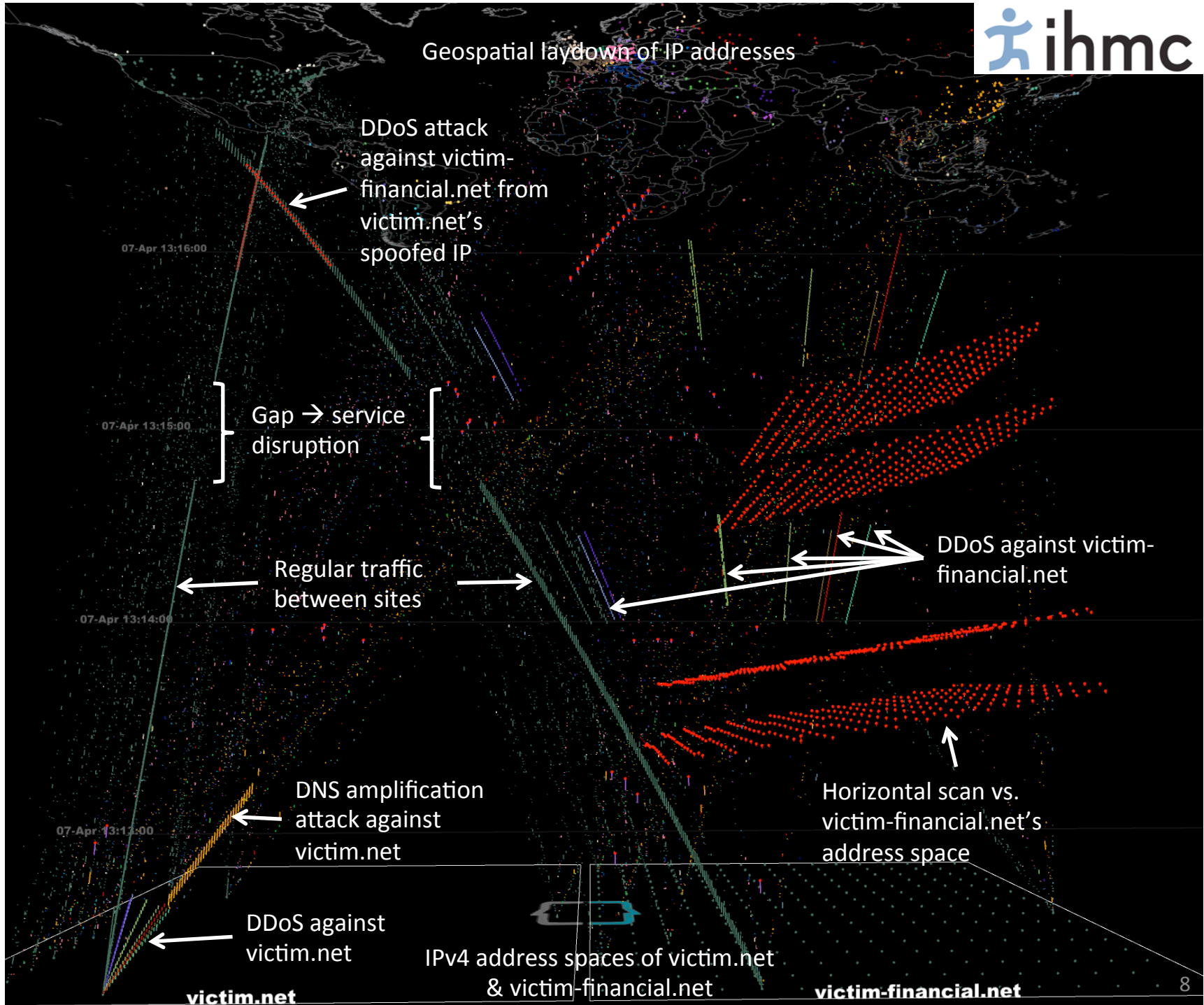


Attacker wants to disrupt the operations and damage the reputation of Company A, which uses Company B's DB service for financial transactions.

- Vignette 1
 - Attacker attempts a Denial of Service attack against Company A.
 - The attack fails, because of Company A's load-balancing infrastructure.
- Vignette 2
 - Attack also knows Company A's web site uses Company B's database service for financial transactions
 - Attacker successfully launches a DoS attack against Company B's database server
- Vignette 3
 - Company B shuts down traffic from attacking DoS IPs
 - Attacker initially believes DoS attack against B is successful, but double checks and finds A's web site still functioning
 - Attacker learns a new potential response/effect to a DoS attack is a blocked IP
 - Attacker formulates a new DoS attack from B to A by spoofing B's IP address
 - B responds by blocking traffic from A
 - Attacker verifies that A's web site is non-functioning



Vignette 3 Example



SC2RAM Cyber Attacker Demo

Vignette 1 Vignette 2 **Vignette 3** Launch Cyber Attack Agent

damage-reputation			
disrupt-operations	disrupt-consumer-webs...	get-ip-number-for-uri	nslookup
		horizontal-scan	
		vertical-scan	
		deny-service	bot-net-dos-attack
			bot-net-dos-attack
disrupt-ecommerce-ser...	disrupt-service-source	get-ip-number-for-uri	nslookup
		vertical-scan	
		deny-service	bot-net-dos-attack
	check-service-attack-st...		
	analyze-goal-failure		

Instead of shutting down their server, Company B blocks traffic from the attacking IPs. Attacker initially believes DoS attack has succeeded. But a double-check finds that the service is still functioning.

Learning from an unexpected goal failure

```
New achieved goal: disrupt-service-source [S17] (subgoal of disrupt-ecommerce-service [S16])
  35:    O: 042 (execute-command)
Executing command check-service-attack-status with argument ^command-argument e-commerce-organization-
b
Executing command check-service-attack-status with argument ^from-goal S16
SIMULATING command check-service-attack-status with argument e-commerce-organization-b: attack failed
Result S16 ^service-attack-failed e-commerce-organization-b created by command check-service-attack-st
atus
Executing command check-service-attack-status with argument ^added-to-gui true
Analyzing unexpected goal failure: subgoal disrupt-service-source achieved, but supergoal disrupt-ecom
merce-service failed on double-check
New active goal: analyze-goal-failure [K10] (subgoal of disrupt-ecommerce-service [S16])
  36:    O: 044 (set-failure-root-goal)
set-value: Root cause of incorrect achievement was goal deny-service
  37:    O: 045 (set-actual-effect)
set-value: Actual effect of goal deny-service was disrupt-service-channel
  38:    O: 047 (learn-projected-effect)
set-multi-value: Learning that a new potential-effect of deny-service is disrupt-service-channel
Creating goal disrupt-service-channel because we have a method (deny-service) to accomplish it
  39:    O: 048 (create-subgoal)
New active goal: disrupt-service-channel [S26] (subgoal of disrupt-ecommerce-service [S16])
  40:    O: 049 (execute-command)
```

o s1

Goal-effect knowledge prior to learning:

(<k> ^goal <kg1>)

(<kg1> ^name deny-service

^potential-effect disrupt-service-source)

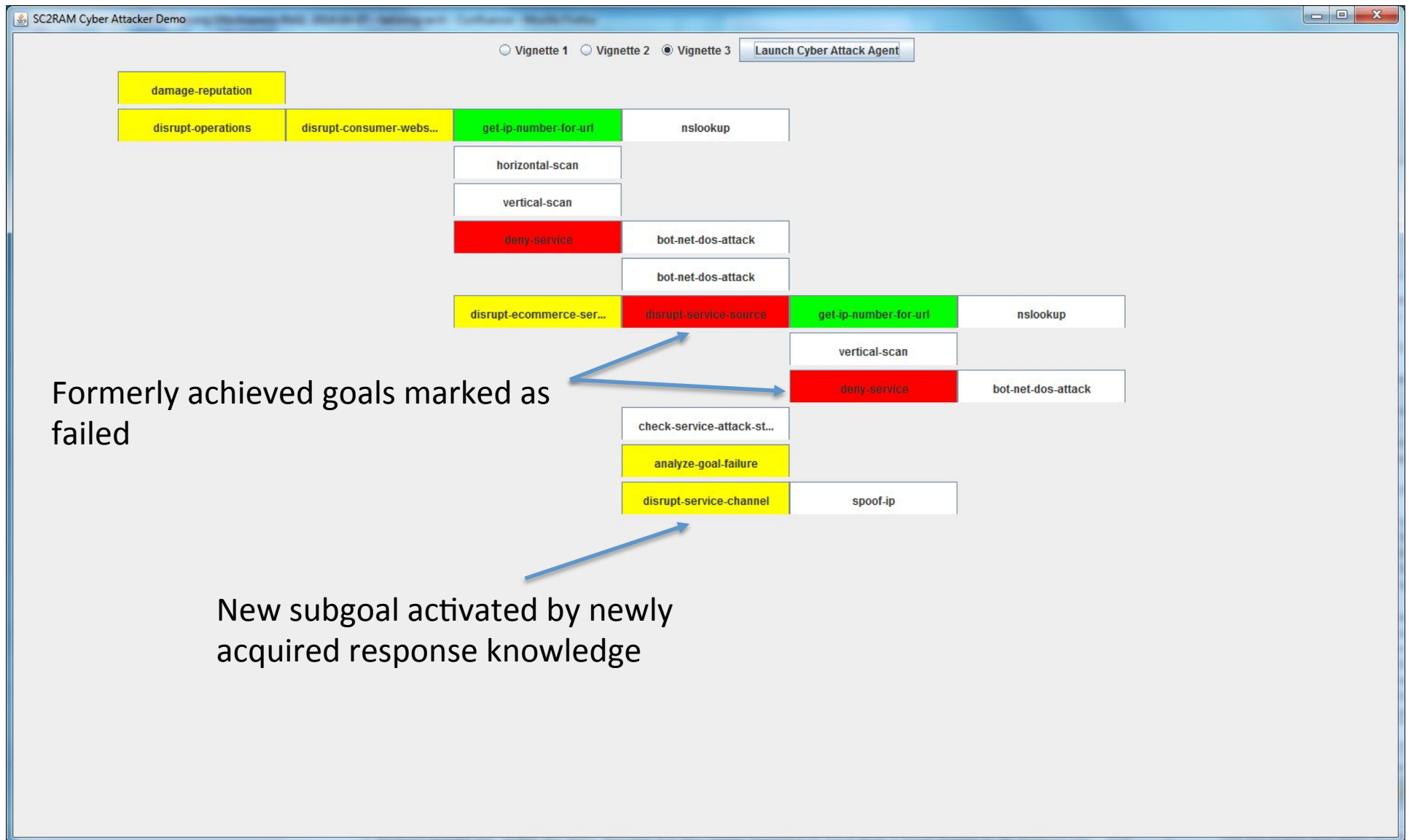
After learning:

(<k> ^goal <kg1>)

(<kg1> ^name deny-service

^potential-effect disrupt-service-source

^potential-effect disrupt-service-channel)



Nuggets

- Soar is well suited to the needs of modeling cyber operations
 - Adaptive
 - Innovative
 - Communicate with others
- Connection with real systems can be facilitated by hybrid architectures
 - IHMC's ontological reasoning for processing low-level NW events
- Strategic potential of collocation of Soar Lab, SoarTech, and Merit/MCR

Lumps

- Current knowledge is very simple, just a prototype
 - SMP
- Knowledge updating requires a Soar programmer
 - Opportunity for interactive task learning