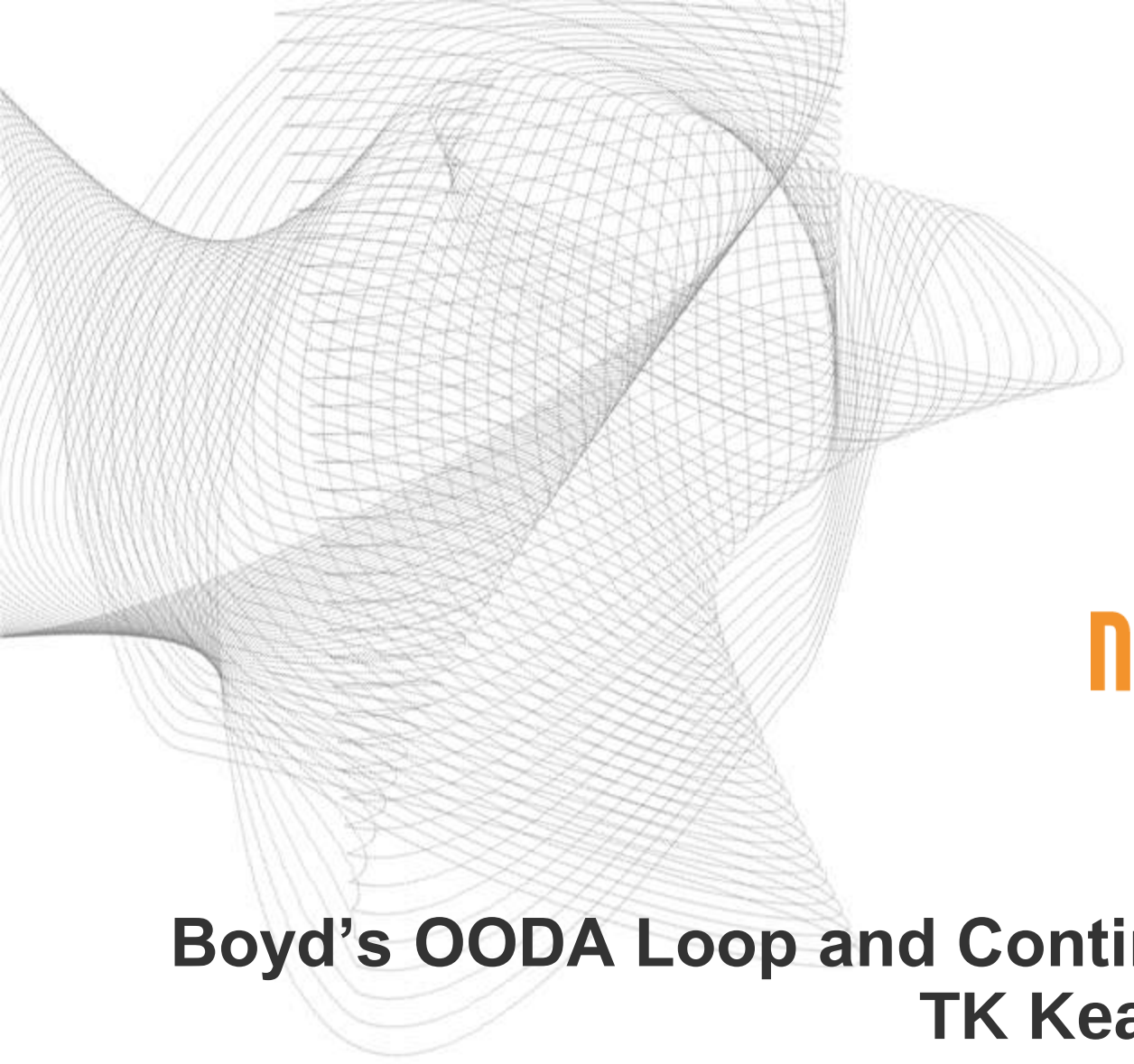


Boyd's OODA Loop and Continuous Monitoring

TK Keanini, nCircle CTO

IT Security Automation Conference, Oct 31, 2011

Hyatt Regency in Crystal City, Virginia

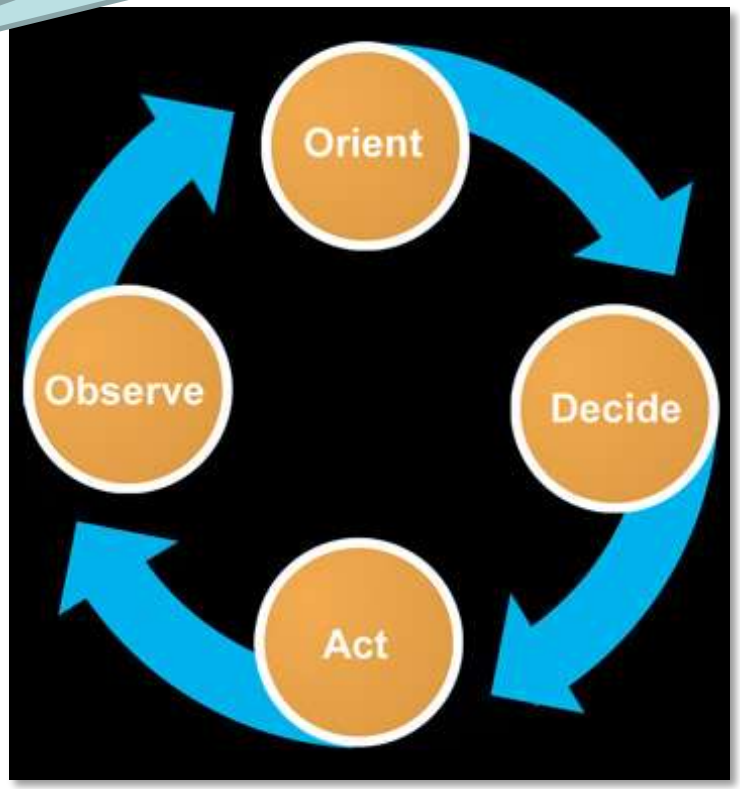
Colonel John Boyd (1927 – 1997)

- Fighter Pilot
  - Forty-Second Boyd
- Military Theories
  - Energy Maneuverability Theory
    - Drove requirements for the F15 and F16
  - Discourse on Winning & Losing
  - Destruction & Creation
  - Many modern military strategies based on Boyd
- The OODA Loop
  - the concept that all combat, indeed all human competition from chess to soccer to business, involves a continuous cycle of Observation, Orientation, Decision, and Action

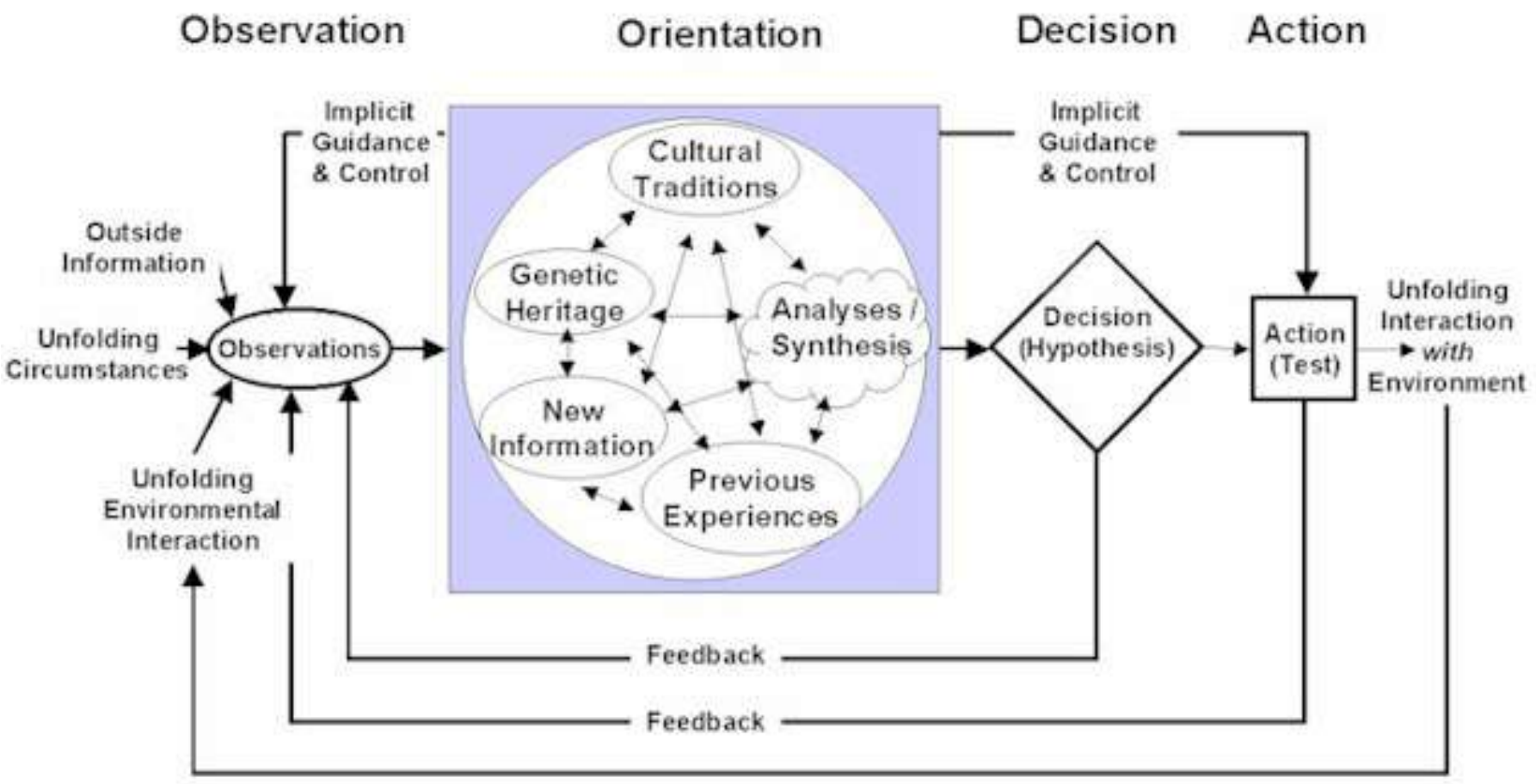
Simplified OODA in the Context of Time

Continuous Monitoring

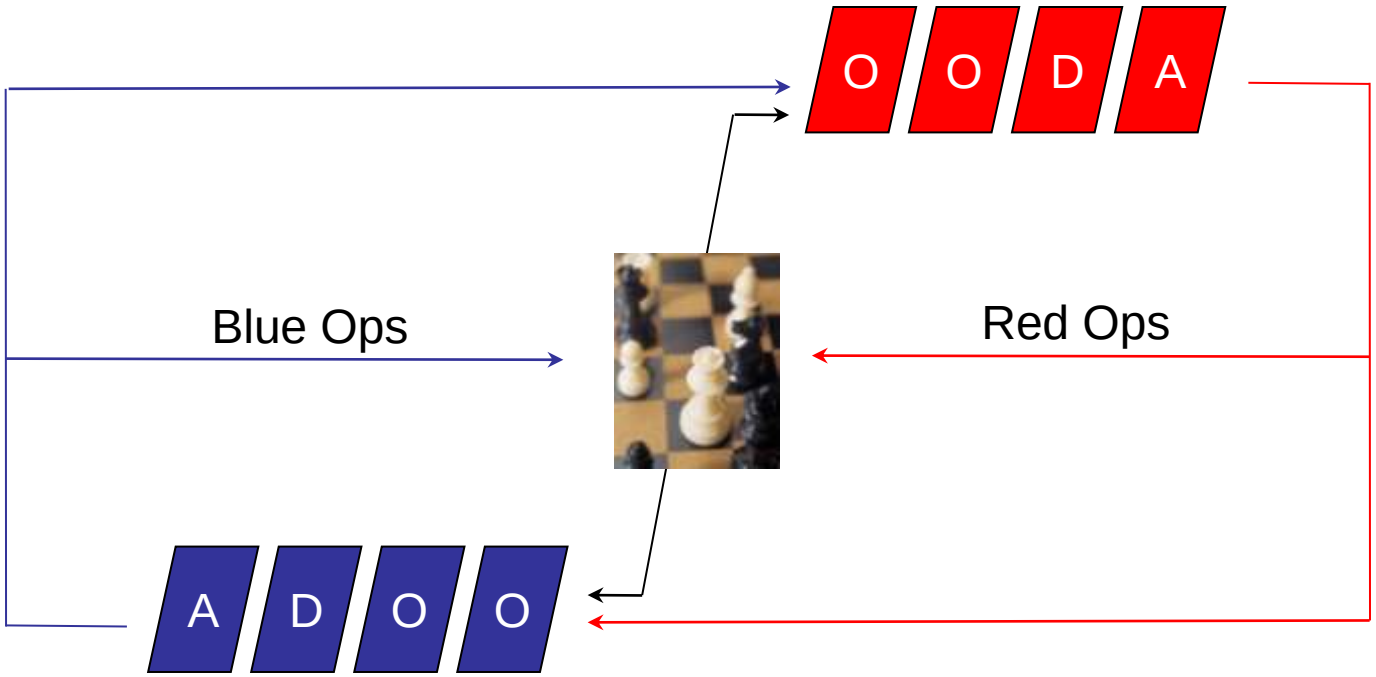
- Intelligence
  - — Observation
  - — Orientation
- Execution
  - — Decision
  - — Action



Feedback Loops of the OODA Loop

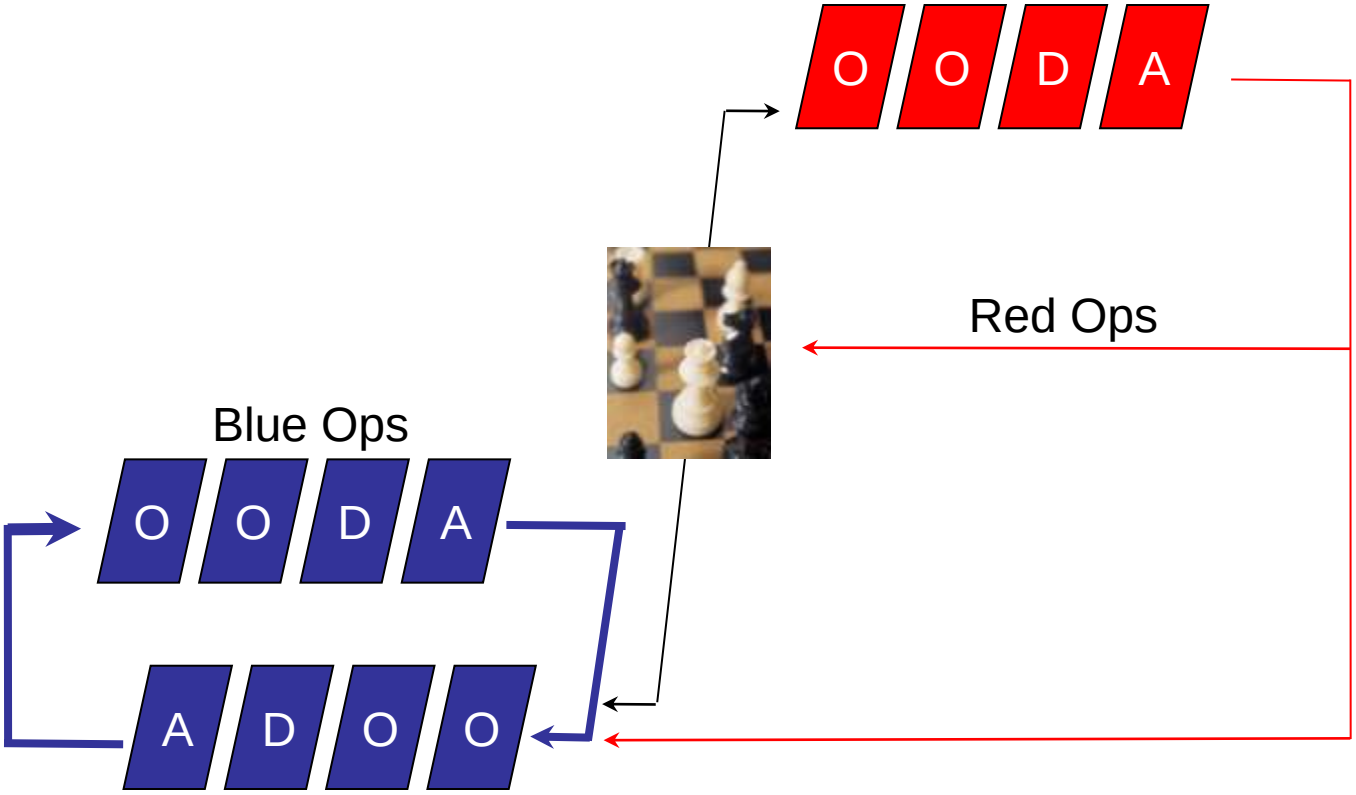


Conflict: Red vs. Blue



Problem:
IT has no offense and cannot act on its adversary

OODA for IT Security



Continuous Monitoring and Rapid Change

Continuous Monitoring/ OODA Loop

- Observation and Orientation (OO) increases your perceptive boundaries.
  - Superior Situational Awareness
- Sampling Rate of the OO is relative to the rate of change
- Your Decision and Actions should drive your rate of change
- Your rate of change should be beyond the perceptive boundaries of your adversaries Observation and Orientation.
  - Actively monitor for this knowledge margin

What is the Objective of your Defensive Strategy?

The primary objective of your IT strategy is:

A) Business continuity and agility?

B) Catching crooks and crime fighting?

IT Security has no direct offensive measures so its dominant strategy must follow that of a prey species!

How can we raise the cost to our predators/adversaries?
(without raising our own costs)

Foraging Patterns of Predator Species

- Cruising (widely foraging)
  - Continually move to locate prey

Dominant strategy back in the day. Servers were the targets and you had to find them

- Ambush (sit-and-wait)
  - Rely on prey's mobility to initiate encounters

With the proliferation of browsers, the prey became mobile and server could ambush

- Saltatory (hybrid)
  - Very little exposure when cruising
  - Cheap ambush resources

Phishing, DNS poisoning, CA spoofing, etc.

Defensive Patterns of Prey Species

- High space and time costs
  - Locations not easily found
  - Location at a high energy cost to predator
- Tolerance
  - Divert the predator to eat non-essential parts
  - Enhanced ability to rapidly recover from the damage
- Befriend your predator's enemy
  - Attract the presence of your predator's predator
- Confrontation
  - Mechanically or chemically

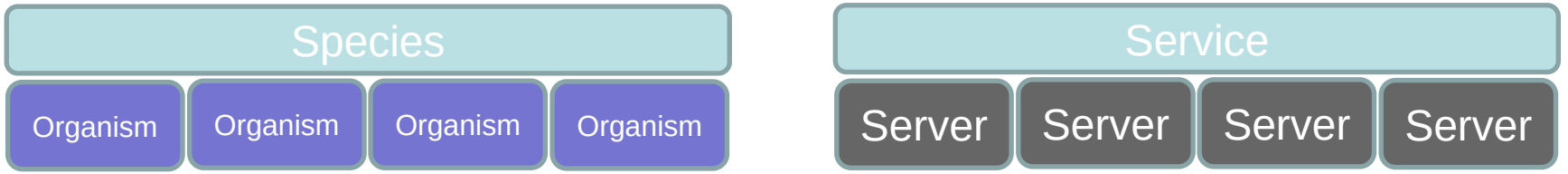
Anti-Predator Strategies (cost/benefit)

- Cost of identification & misidentification
  - Camouflage
  - Overtly advertise negative benefits
- Cost of attack
  - Energy gained from the kill / energy spent in the hunt
- Cost of handling/ingest
  - Energy spent to convert
  - Lifetime of the gain

Loss is a part of the design

The Organism is the target, not the Species

The Patterns of a Prey Organism



- The game of *survival* and *resiliency* is at the level of *species* and not at the level of *organism*
- Diversity, redundancy and a high rate of change at the organism level provides stability at the species level
- Loss at the organism level is informational
- With no offensive measures, prey must advertise unprofitability and raise the cost to its opponent

Change is Not Happening Fast Enough!

- Server A is configured, tested, and put in to production
- In a 96 hour period, your adversary is able to perform enough recon to pick a strategy
- Server A will remain in that original production state until
  - A change is required by the business
  - A change is required by the discovery of a vulnerability
  - A change is required by a fault
  - Otherwise, it remains the same for what could be months or years (prime real estate for a parasite)
  - Can't eat just one! What works on A will work on B through 'n'

The adversary will take advantage of the fact that your cost of change is too high

Decoupling Organism from Species

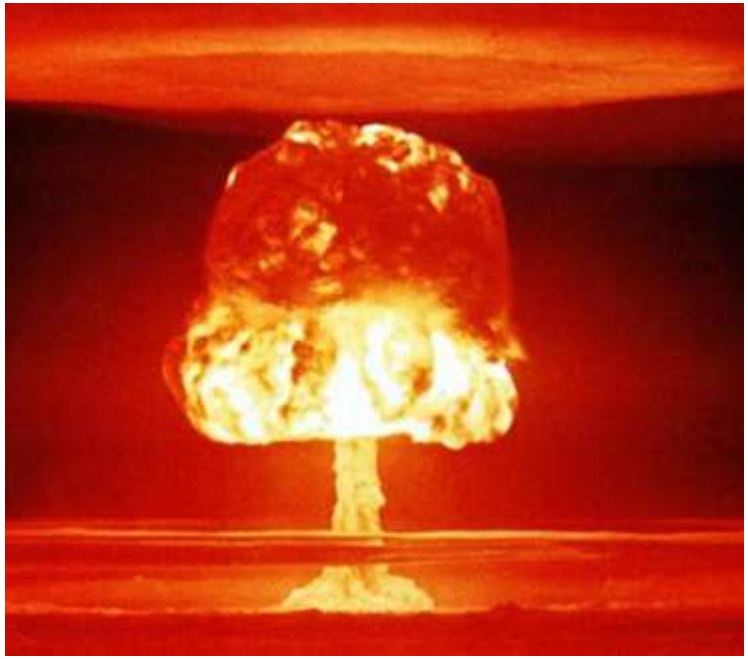
Pattern: The abstraction of a [re]source

A few examples include:

Virtual LANS	Logical partitioning of broadcast domains
Virtual Storage	Logical presentation of disks
Virtual Service	Load Balancers, Proxies, etc.
Virtual Machines	VMware, Xen, Microsoft's Virtual Server, etc

Advantage: Decoupling the resource from the source

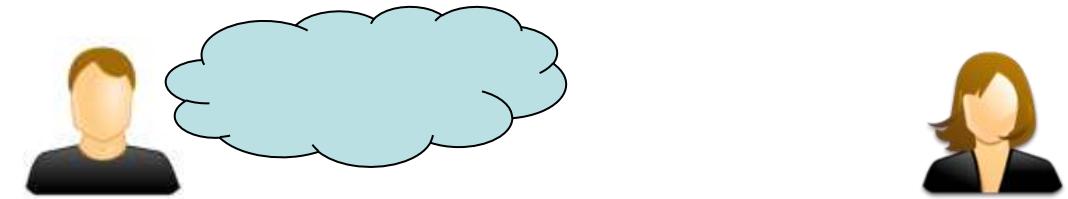
Nuke & Pave



What if we could lower the ‘Mean Time to Recovery’ of the service to seconds?

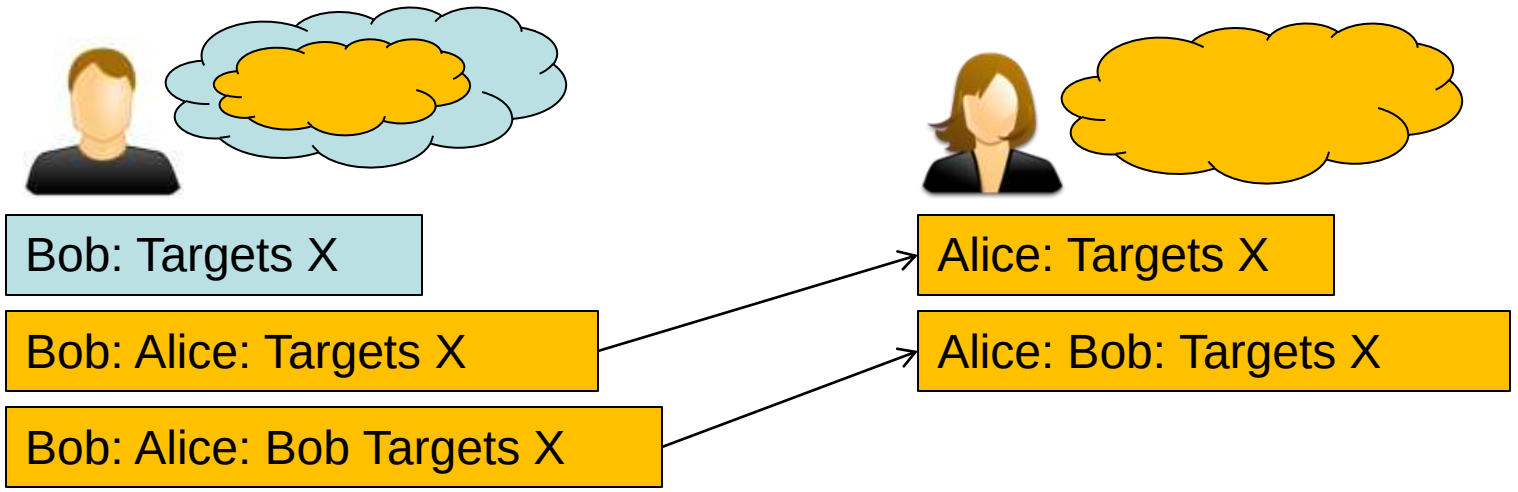
What if we could change characteristics in the server while keeping the service the same?

Orientation: Information Sets



- Ego-centric understanding
  - What you know about your targets

Orientation: Information Sets



- Allo-centric understanding
  - — What you know, what your opponent knows about your targets
  - — What you know, what your opponent knows, what you know about your targets.

The cost of your adversaries Observation and Orientation (OO)

- Your common target attributes
- Your common practices
- Your High Cost of Change: MTTR (Mean Time to Repair) or TTM (Time to Manufacture)
- How can we lower the effectiveness of their tools or process?
- How can we raise their costs?

Knowledge Margin

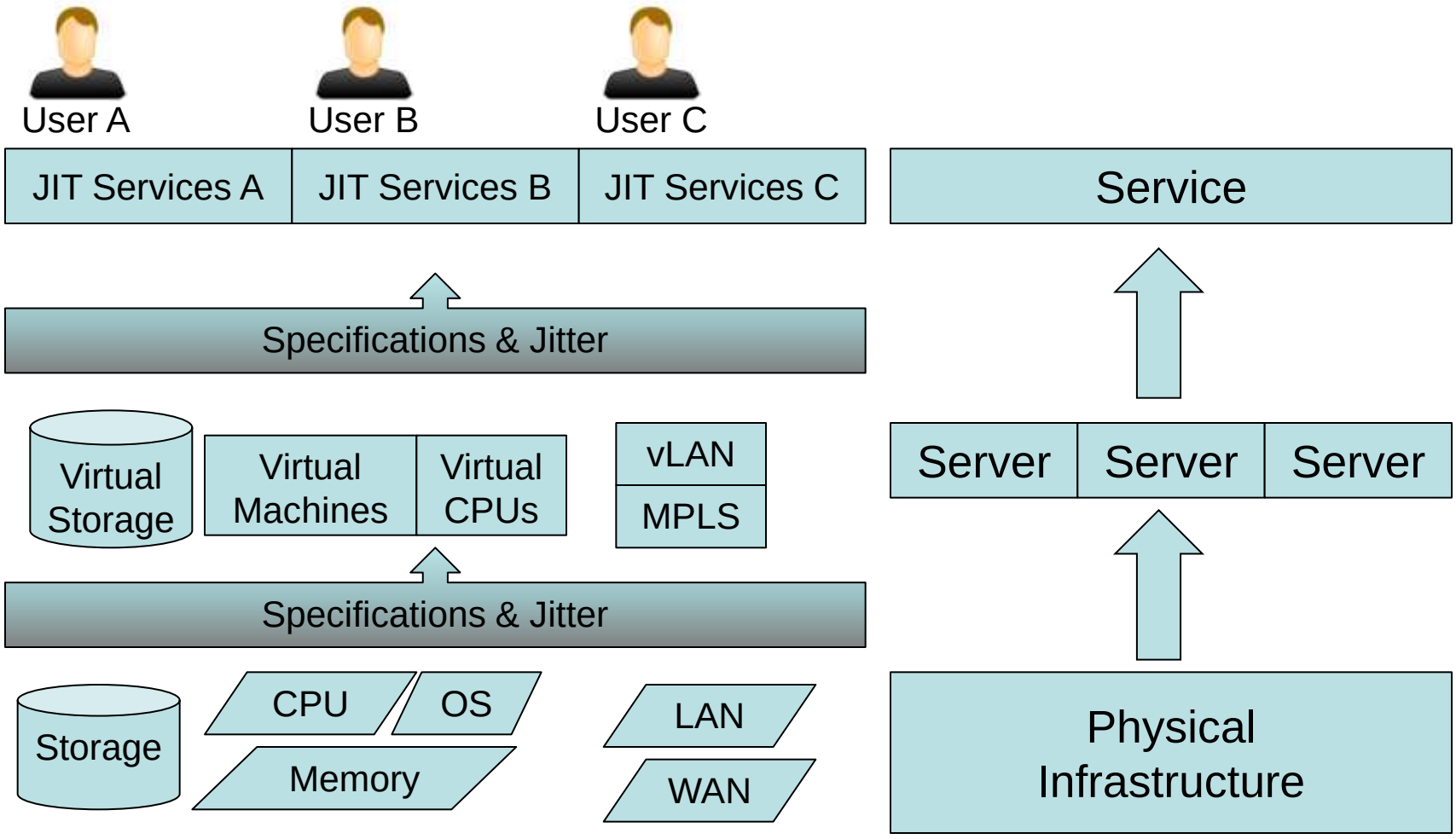
$$\frac{dTarget}{dTime} \succ \frac{dAdversary\ Observation}{dTime}$$

"If a target system can cause the adversary to constantly have to recompute their tactics, to cause uncertainty on the adversary's causal models, they can achieve a knowledge margin that is feasible and sustainable." - TK

Creating a Knowledge Margin

- Leverage virtualization for synthetic provisioning
- Ability to provision the entire ‘backend’ on a per session basis
- Continuously monitor for diversity without adding administrative costs

Example: Synthetic Provisioning



Continuous Monitoring/ OODA Loop Summary

- We must find a way to **raise the cost to our adversary** while not raising our own administrative costs
- Observation and Orientation (OO) increases your perceptive boundaries.
- Sampling Rate of the OO is relative to the rate of change
- Your Decision and Actions should drive your rate of change
  - Proactively introduce change at the server level while holding to your service level agreements
- Your rate of change should be beyond the perceptive boundaries of your adversaries Observation and Orientation.
  - Actively monitor for this knowledge margin

Contact

Twitter: @tkeanini

tk@ncircle.com