Mission Models: bridging kinetic & cyber warfare

HARRIS®

Ronda Henning   Wayne Smith
rhenning@harris.com   wsmith029@harris.com

In the Cyber Domain

- Build a Defense in Depth model, and hope the walls hold.
- Mobility and Agility are the enemy of the fortress
- How can you provide resilient cyber operations anywhere, anytime?

Comparison of Cyber Warfare Strategies

HARRIS

|	**Attrition**	**Maneuver**
Definition	Collection of targets to be found and destroyed.	Isolation of adversarial forces and the exploitation of their weaknesses by movement
Terrain and Tactics	Static fortifications determine battlefield terrain and battle rhythm – allows adversary to reconnoiter and attack.	Maneuver strategy controls the terrain and battle tactics – prevents enemy reconnoiter and effective attacks
System Architecture	Defense in Depth	Dynamic, turbulent and disruptive; chaotic
Basic Strategy	Attack till breached	Shatter adversary's offensive ability to find targets

OODA Loop Concepts

Event Stimulus → **Response Action**

Response Time

Observe (Event) → **Orient** → **Decide** → **Action**

Response Time

Observe (Event) → **Orient** → **Decide** → **Action Response**

Response Time

Observe (Event) → **Orient** → **Decide** → **Action Response**
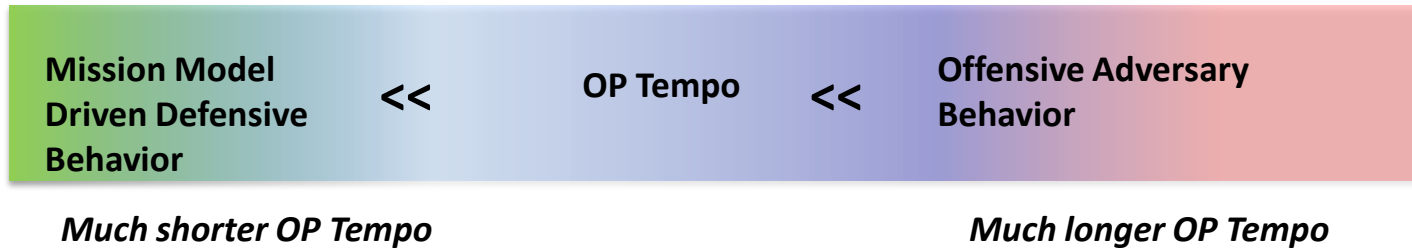
Response Time

Boyd's OODA Loop: The OODA loop is the process we go through in responding to an event stimulus.
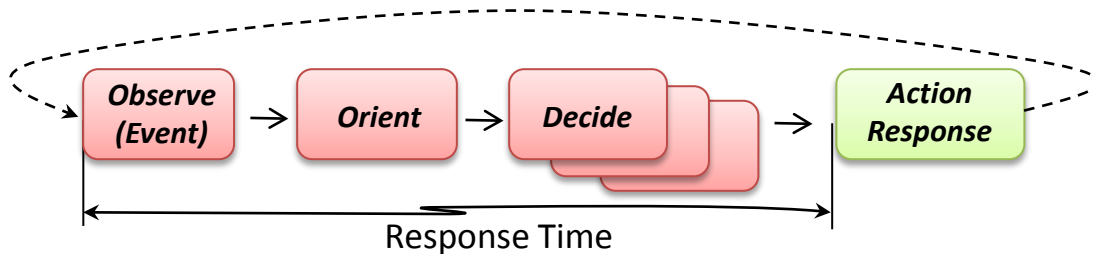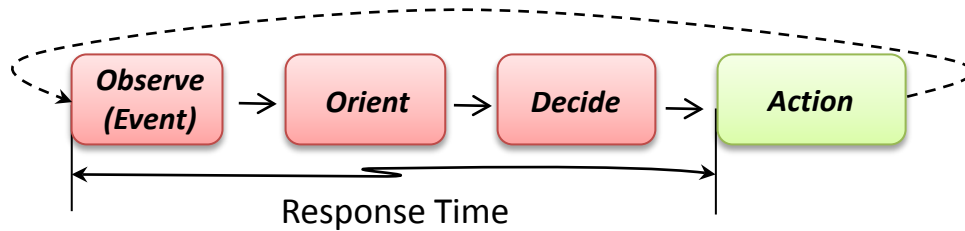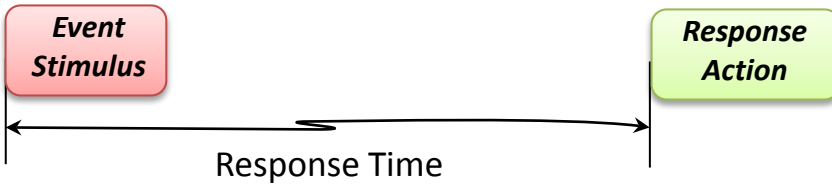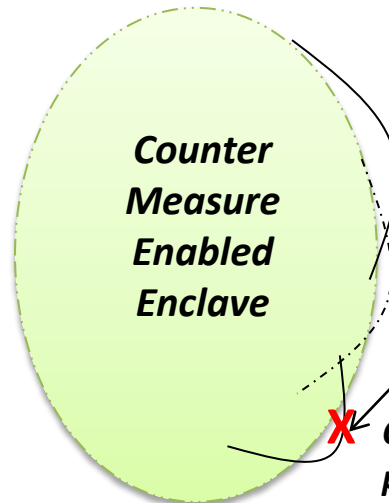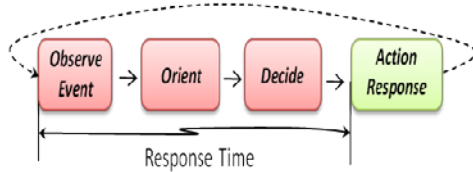
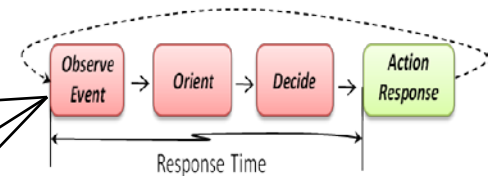**_Hick's Law:_** Multiple decisions extend response time by 58%.
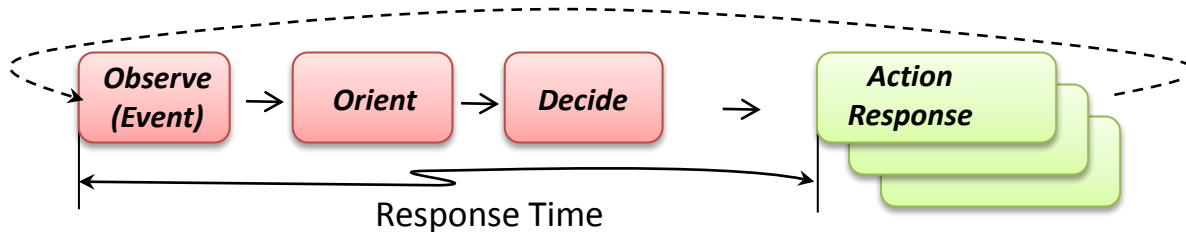
Henry & Rodgers: Multiple responses and increased complexity of responses extend response time by 31%.

Command and Control Concept for Cyber

HARRIS

Mission Model Driven Defensive Behavior	<<	OP Tempo	<<	Offensive Adversary Behavior

Much shorter OP Tempo   *Much longer OP Tempo*

Defensive OODA

Counter Measure Enabled Enclave

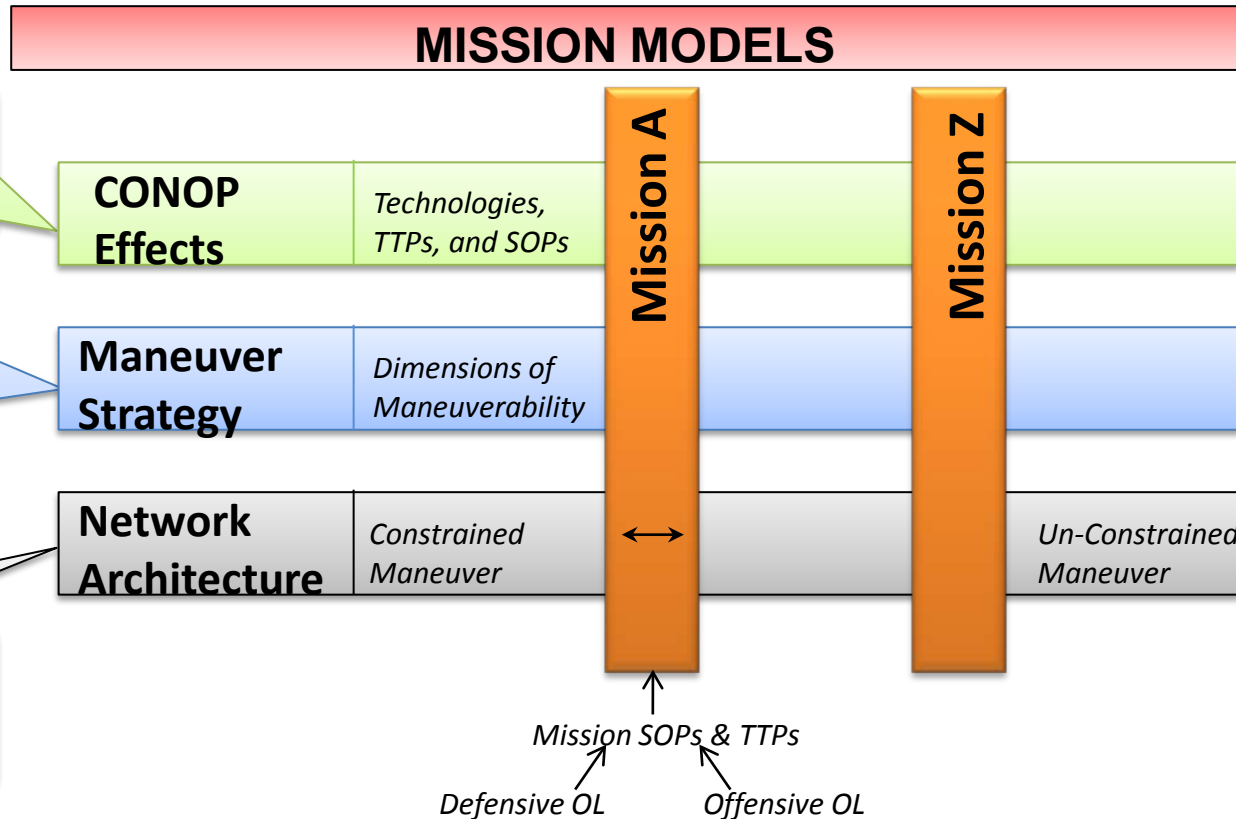## Offensive OODA

Cyber attacks do not reach protected assets.

- Adversary uses their proves static attack doctrine, SOP's, and TTP.
- Adversary observes static data within reconnaissance efforts
- Adversary orients to static target
- Adversary actions fail AND adversary unwittingly reveals intentions

Relationship

MISSION MODELS

Analyze and design the effects desired to impact the offensive adversary's decision making and actions (OODA Loop).

Develop the Maneuver Strategy that will produce the desired or needed effects for the operator
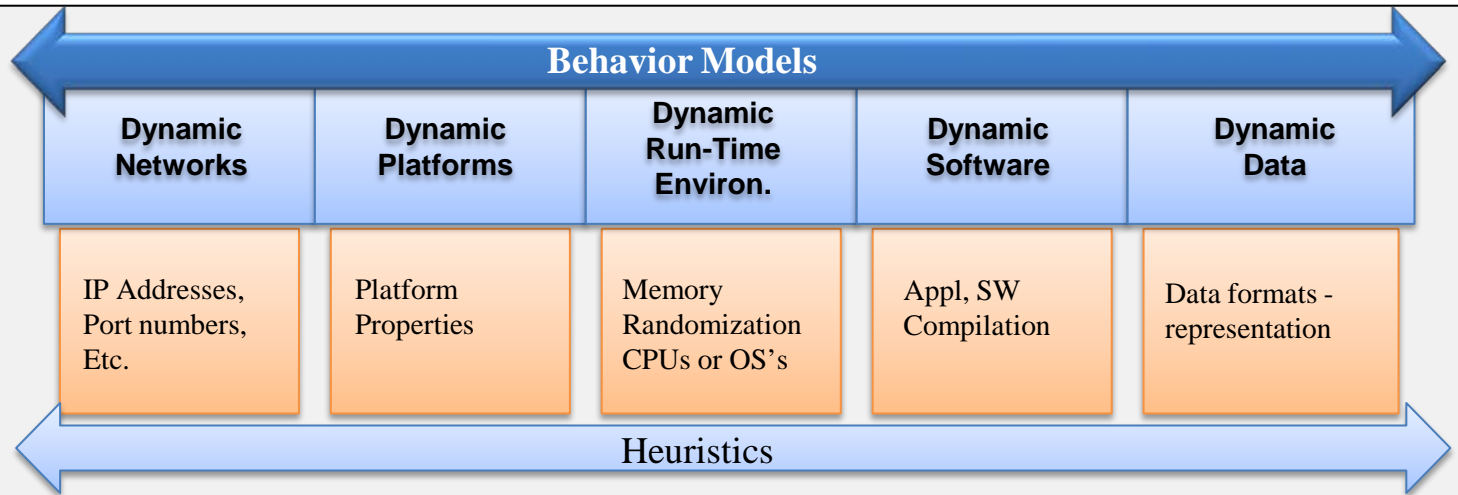
Determine the required network architecture and the maneuver constraints that the mission must operate within

		Mission A		Mission Z
CONOP Effects	*Technologies, TTPs, and SOPs*			
Maneuver Strategy	*Dimensions of Maneuverability*			
Network Architecture	*Constrained Maneuver*	↔		*Un-Constrained Maneuver*

Mission SOPs & TTPs

Defensive OL   *Offensive OL*

For each mission, there is a relationship between CONOP, Maneuver Strategy, and Network Arch.
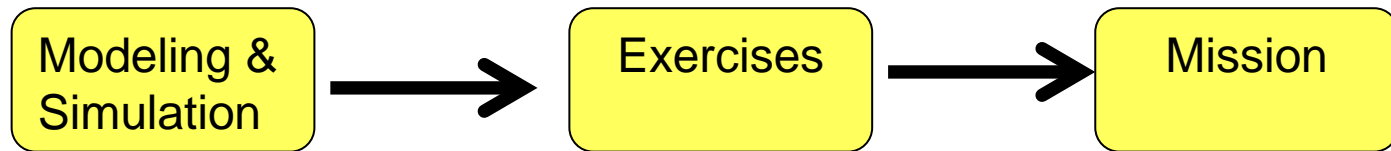
The Maneuver Strategy and corresponding Dimensions of Maneuverability must take into account the network architecture and boundaries associated with constrained vs. un-constrained maneuverability for the mission.

The Maneuver Strategy is designed to produced the desired effects within the offensive adversary's OODA Loop, taking into account the Maneuver Warfare Rules.

The Mission Models

Desired Objective: Delay, Deter, Detect Adversary

Cyber Domain Adapted Maneuver Warfare

Behavior Models

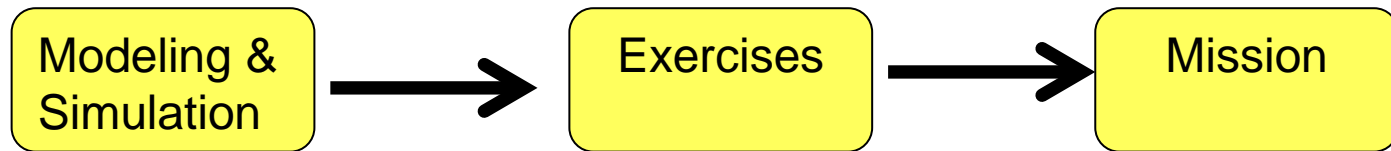| **Dynamic Networks**	**Dynamic Platforms**	**Dynamic Run-Time Environ.**	**Dynamic Software**	**Dynamic Data**
IP Addresses, Port numbers, Etc.	Platform Properties	Memory Randomization CPUs or OS's	Appl, SW Compilation	Data formats - representation

Heuristics

Mission Models

In Conclusion

- For traditional warfare (sea, land, air, space) domains, we follow a very structured process:

Modeling & Simulation	→	Exercises	→	Mission

- Modeling and simulation provide nondestructive "practice"
- Exercises validate the models and provide "hands-on practice"
- Eventual goal is a successful mission

In the cyber domain, we employ static defenses and hope we are not breached while we fight….

Conclusion (Part II)

- To converge cyber with physical domains, it needs to be incorporated into the process:

```
┌─────────────┐      ┌─────────────┐      ┌─────────────┐
│ Modeling &  │ ───► │  Exercises  │ ───► │   Mission   │
│ Simulation  │      │             │      │             │
└─────────────┘      └─────────────┘      └─────────────┘
```

Mission models provide:
- a way to integrate cyber with traditional warfare planning
- a way to calculate cyber impact on specific elements
- a way to improve resiliency
- an integrated operational plan

Being tested in CyberFlag exercises today