Think Like a Bad Guy

Applying the Axioms of Cyber Warfare

A “Perfect Storm” Environment

Primary challenges

1. **Nature and motivation of attack**
   (hacktivist, nation state)
2. **Transformation of enterprise IT**
   (delivery and consumption changes)
3. **Regulatory pressures**
   (increasing risk, cost and complexity)

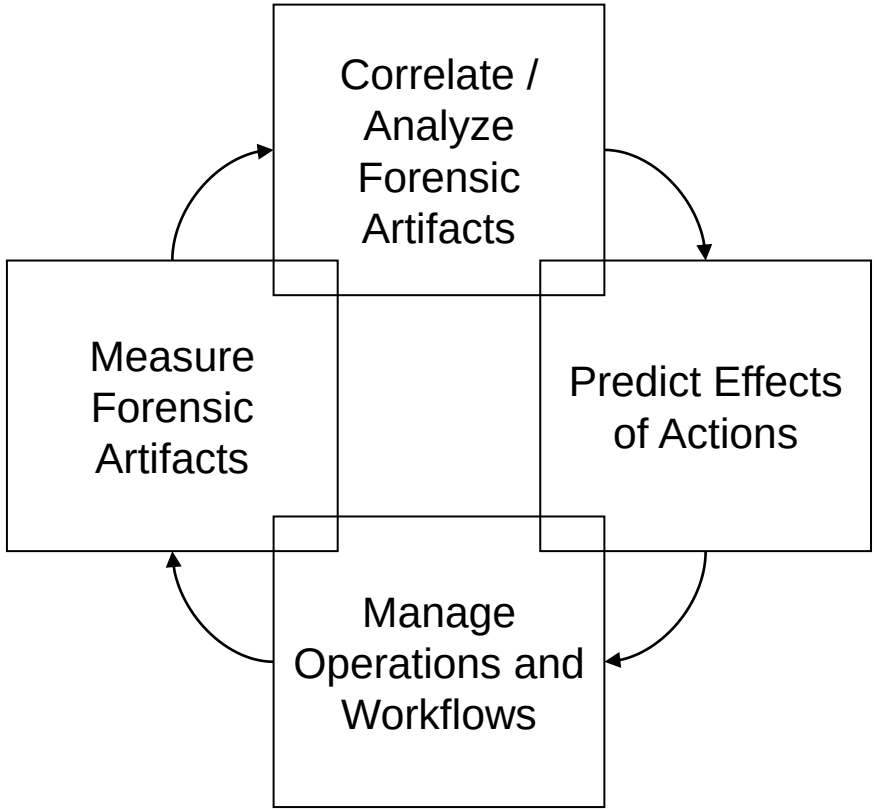
A new type of adversary

Delivery

Enhanced regulatory environment

The Operational View of Attack & Defense

Understand operational artifacts in real-time



Determine business operational risks

Describe, classify and assess a digital environment

Mitigate operational risks
Avoid – Reduce - Transfer

Axioms of Cyber Warfare

- **Access-Driven Phenomenon. Get Lower in Stack to Win**
  - **Application**
  - **Network**
  - **Maintenance**
  - **Procurement**
  - **Manufacture**

Axioms of Cyber Warfare

- Access-Driven Phenomenon. Get Lower in Stack to Win
- **Cyber Warfare is a Mission-Centric Issue**
  - **Prefer engineered solutins**
  - **Avoid event-driven solutions**
  - **Focus on mission assurance in the face of adversary action**

Axioms of Cyber Warfare

- Access-Driven Phenomenon. Get Lower in Stack to Win
- Cyber Warfare is a Mission-Centric Issue
- **Multiple Use Nature of Cyber Resources**
  - **People**
  - **Process & Policy**
  - **Sensors**
  - **Weapons**

Axioms of Cyber Warfare

- Access-Driven Phenomenon. Get Lower in Stack to Win
- Cyber Warfare is a Mission-Centric Issue
- Multiple Use Nature of Cyber Resources
- **Intertwined Technical Relationships**
  - **Readiness & predictability of adversary weapons system**
  - **Health & status of targeted system**
  - **System policy and agility**
  - **System resilience and diversity**

Axioms of Cyber Warfare

- Access-Driven Phenomenon. Get Lower in Stack to Win
- Cyber Warfare is a Mission-Centric Issue
- Multiple Use Nature of Cyber Resources
- Intertwined Technical Relationships
- **Policy is Part of the System - Constraints Drive Outcomes**
  - **Offensive & Defensive Boldness**
  - **Maneuverability & Compliance**
  - **Privacy & sense-making**

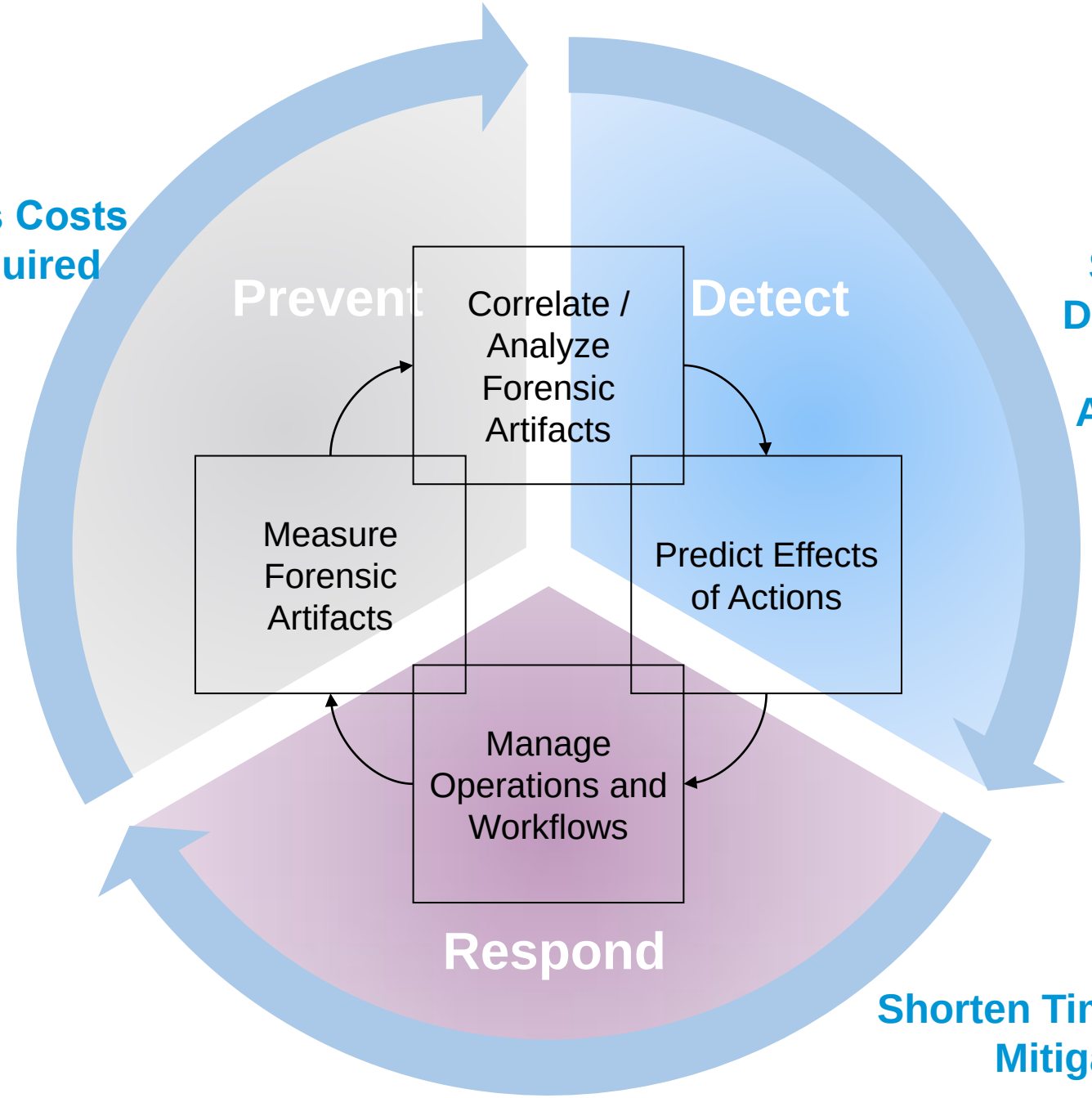
Axioms of Cyber Warfare

- Access-Driven Phenomenon. Get Lower in Stack to Win
- Cyber Warfare is a Mission-Centric Issue
- Multiple Use Nature of Cyber Resources
- Intertwined Technical Relationships
- Policy is Part of the System - Constraints Drive Outcomes
- **Calculate the Higher Order Effects**
  - **Blowback of offensive & defensive action**
  - **Standardization & compliance**

Axioms of Cyber Warfare

- Access-Driven Phenomenon. Get Lower in Stack to Win
- Cyber Warfare is a Mission-Centric Issue
- Multiple Use Nature of Cyber Resources
- Intertwined Technical Relationships
- Policy is Part of the System - Constraints Drive Outcomes
- Calculate the Higher Order Effects
- **Cyber Systems Are Maneuverable Platforms**
  - **Obfuscation for offense and defense**
  - **Complicate the adversary decision space**
  - **Provide options for mission assurance**

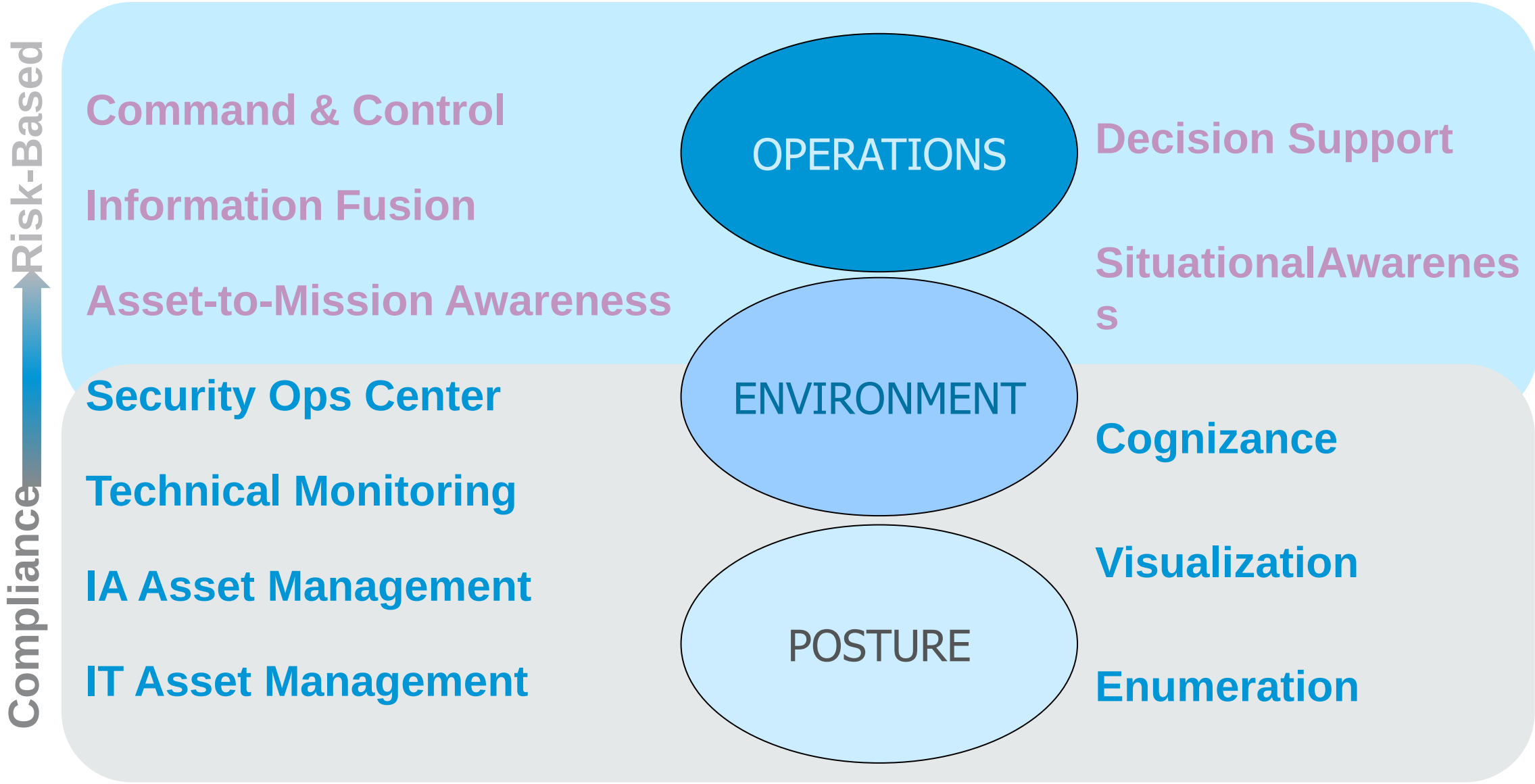
Increase Adversary's Costs
Lengthen Time Required



Shorten Time to Detect and Assess the Impact of Adversary Action

Shorten Time to Disrupt and Mitigate Attacks

A Maturity Model for Cyber-Dependent Operations



Think Like a Bad Guy

Applying the Axioms of Cyber Warfare