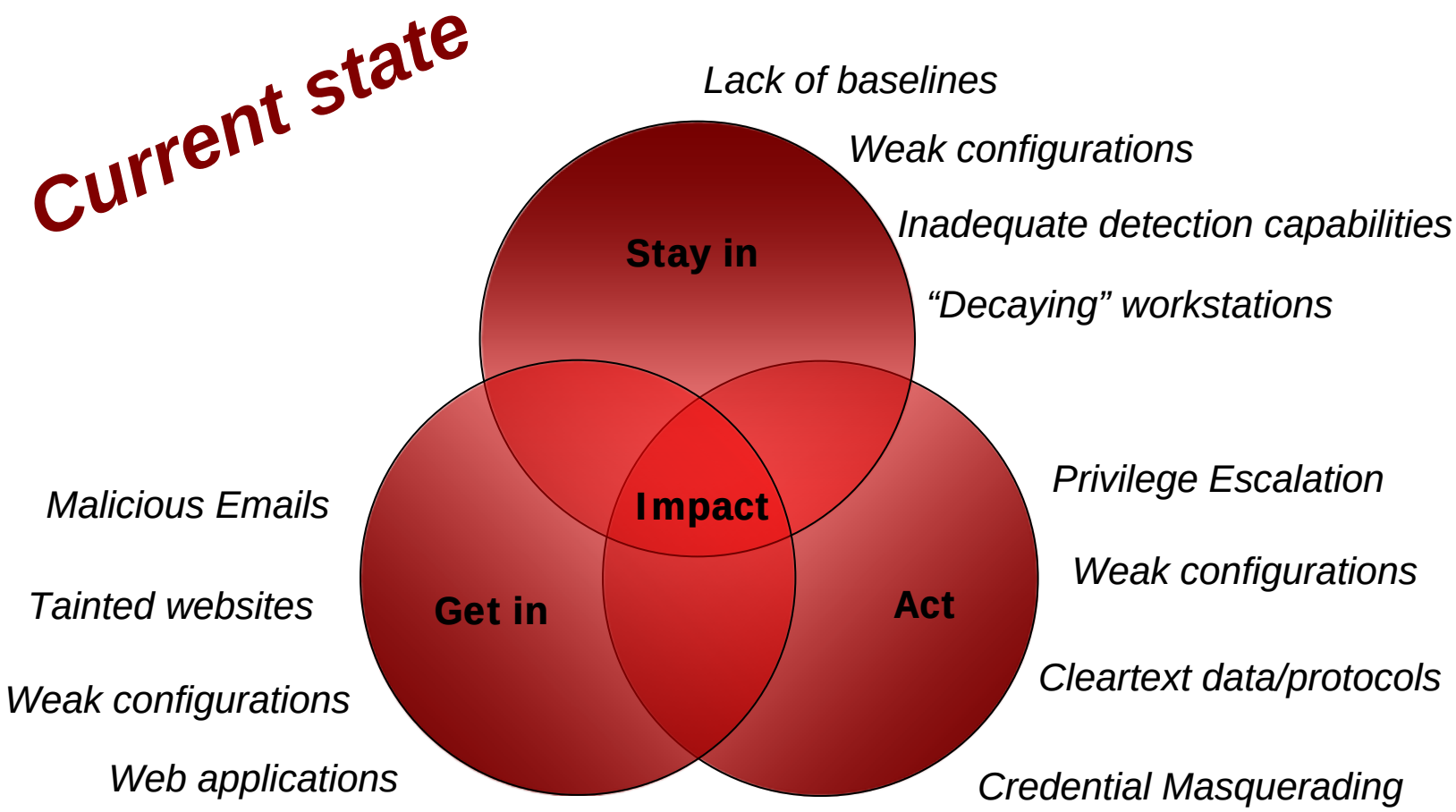
CIO/NII
Enabling Net-Centric Operations

# SCAP Event Standards - Support to Computer Network Defense

## SCAP Conference – October 2009

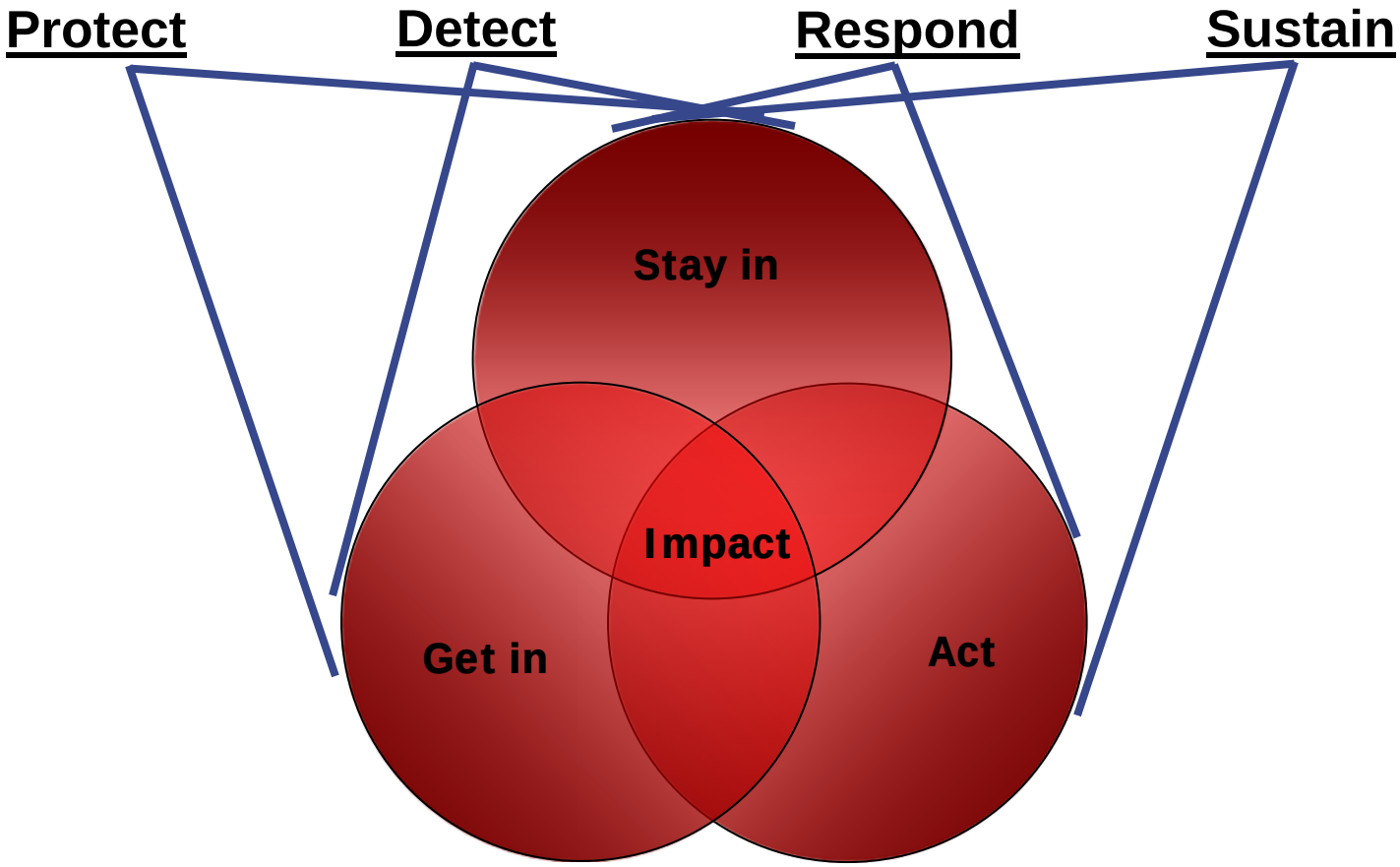

**Kevin Bingham**
**DoD CND Architect**
**Office of DASD for Information and Identity Assurance**

# An adversary's ability to impact




Adversary's ability to impact results from success in all three areas – shrinking any of the circles results in a reduced level of impact

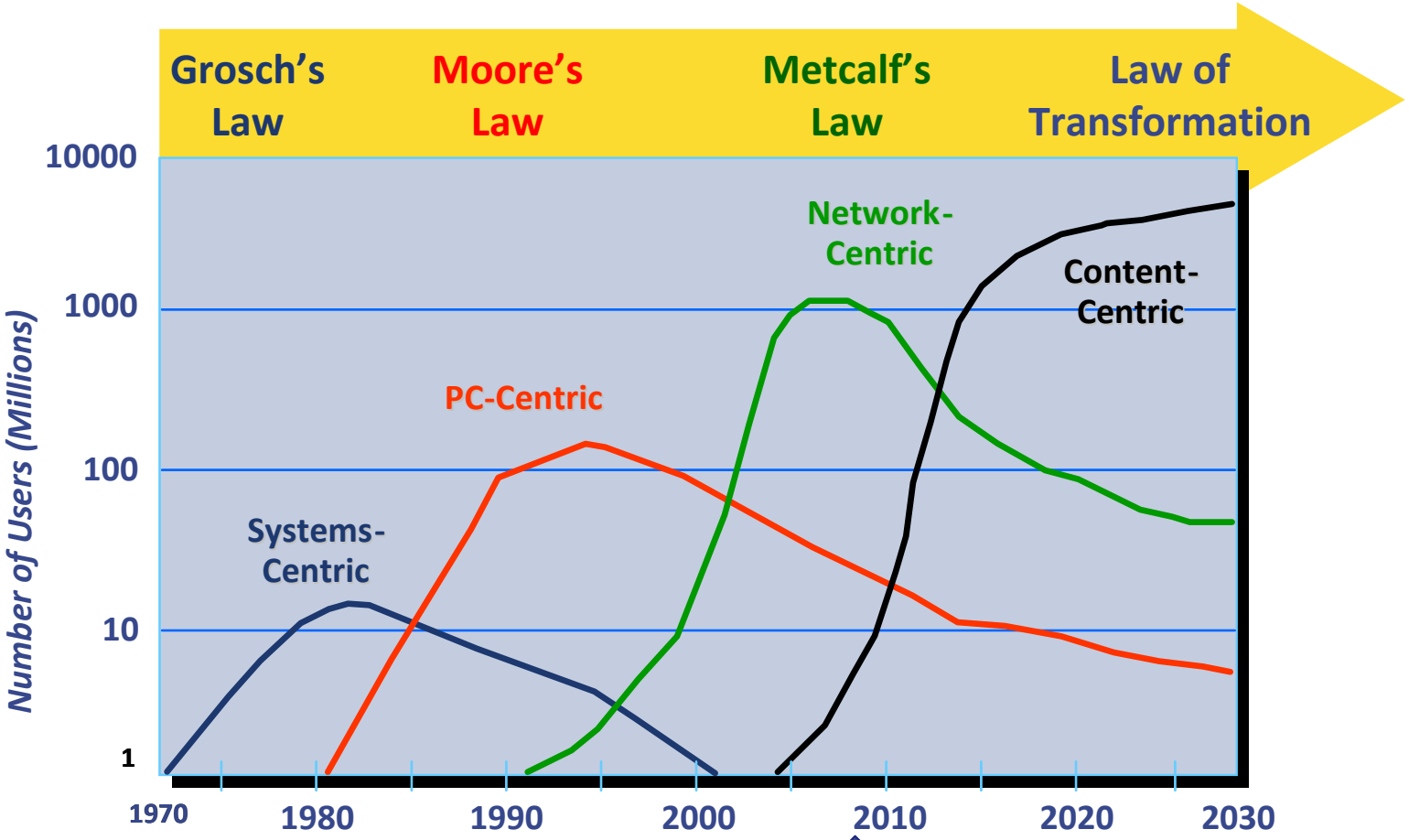
# An adversary's ability to impact




Adversary's ability to impact results from success in all three areas – shrinking any of the circles results in a reduced level of impact

# Looking Ahead . . . Looking Back

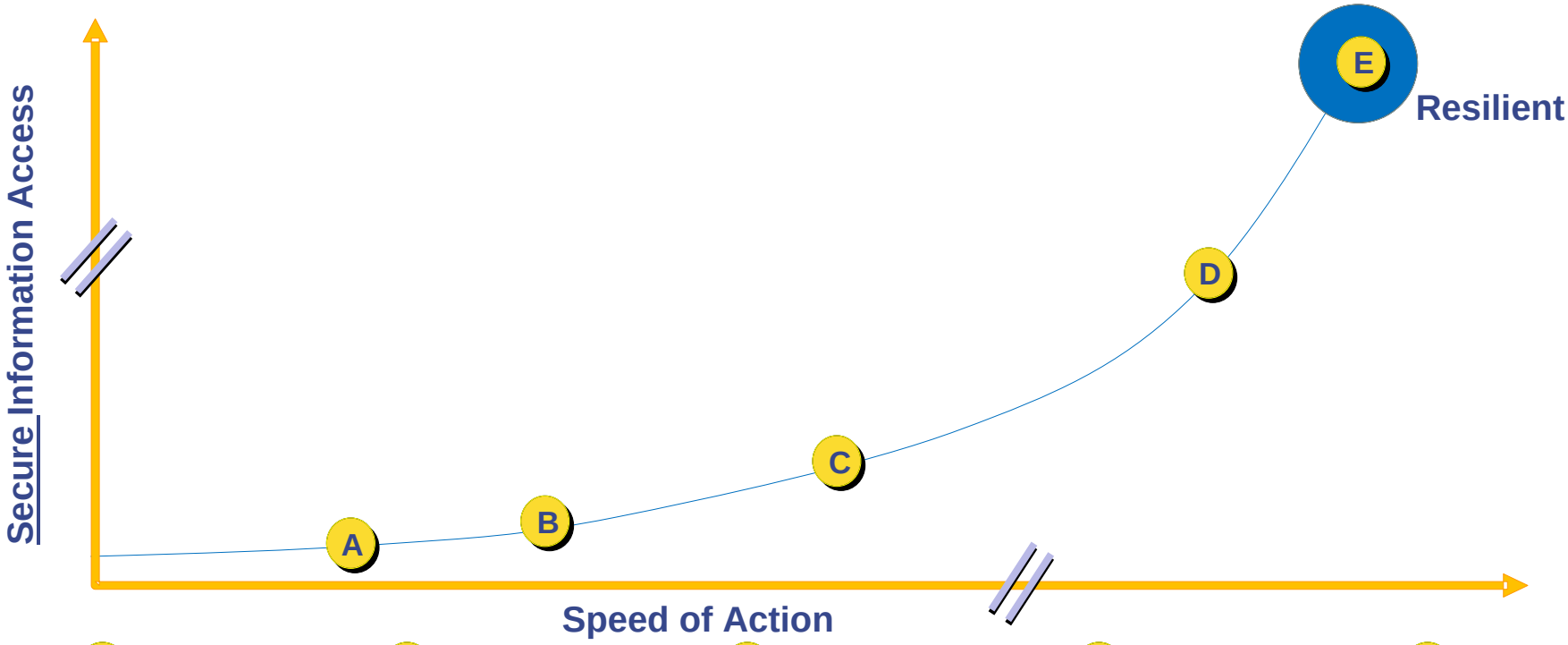
## Waves of IT Industry Growth in the Information Age




*Source: David Moschella, "Waves of Power", 1997*

CIO/NII Enabling Net-Centric Operations

# Toward a Resilient Cyber Ecosystem




**A**

## Reactive & Manual

Security administrators follow rules and do their best to "put out fires"

**B**

## Tools-Based

Tools and technologies are applied piecemeal to assist people in reacting faster

**C**

## Interoperable

Loosely integrated tools exchange data to assist people with cyber situational awareness

**D**

## Policy-Based

The enterprise instantiates security policy, illuminates events and helps the operators find, fix, and target for response

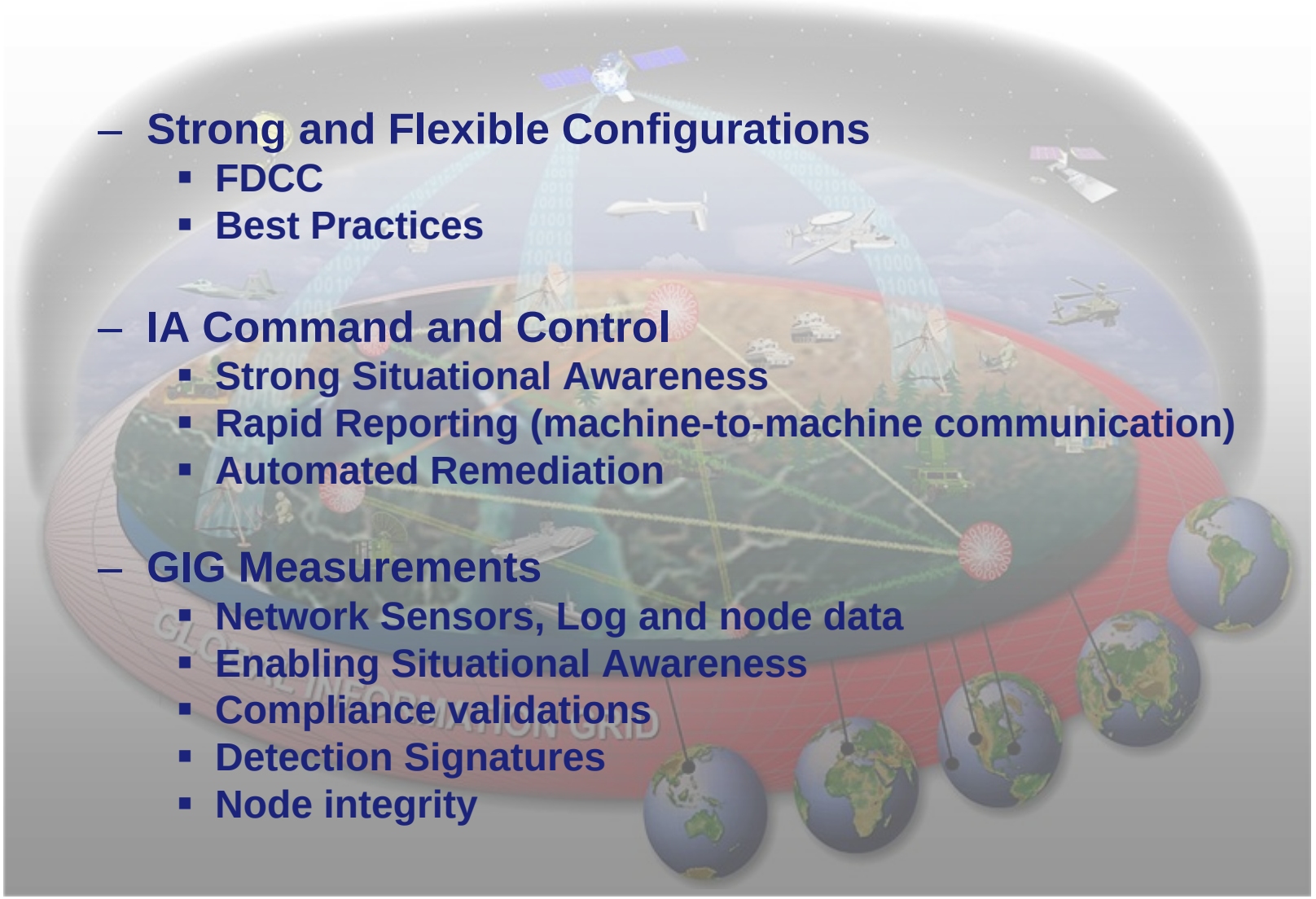
**E**

## Resilient

Enterprise optimizes service to user by to dynamically isolating and containing effects – including in supply chain and underlying infrastructure

# SCAP - Enabling NetOps through

- Strong and Flexible Configurations
  - FDCC
  - Best Practices
- IA Command and Control
  - Strong Situational Awareness
  - Rapid Reporting (machine-to-machine communication)
  - Automated Remediation
- GIG Measurements
  - Network Sensors, Log and node data
  - Enabling Situational Awareness
  - Compliance validations
  - Detection Signatures
  - Node integrity

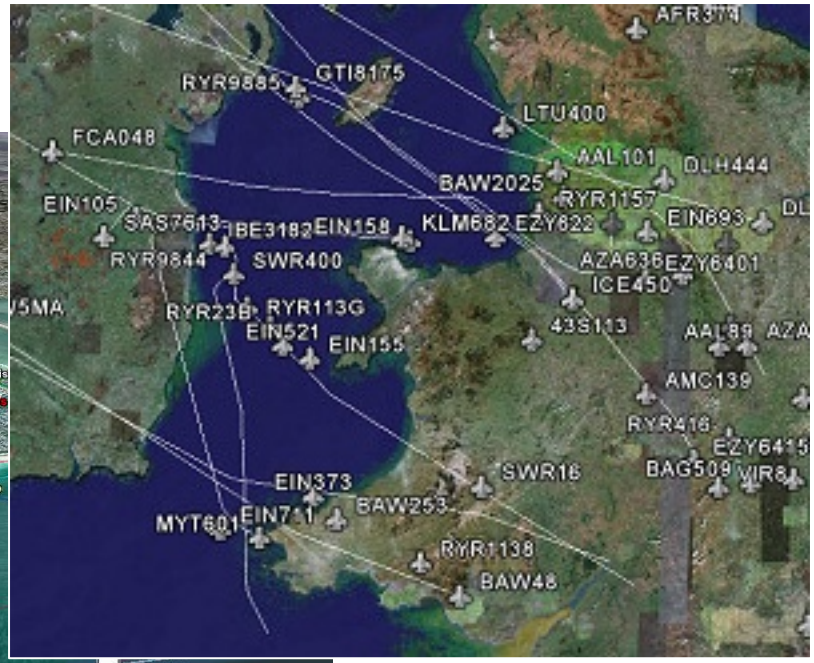


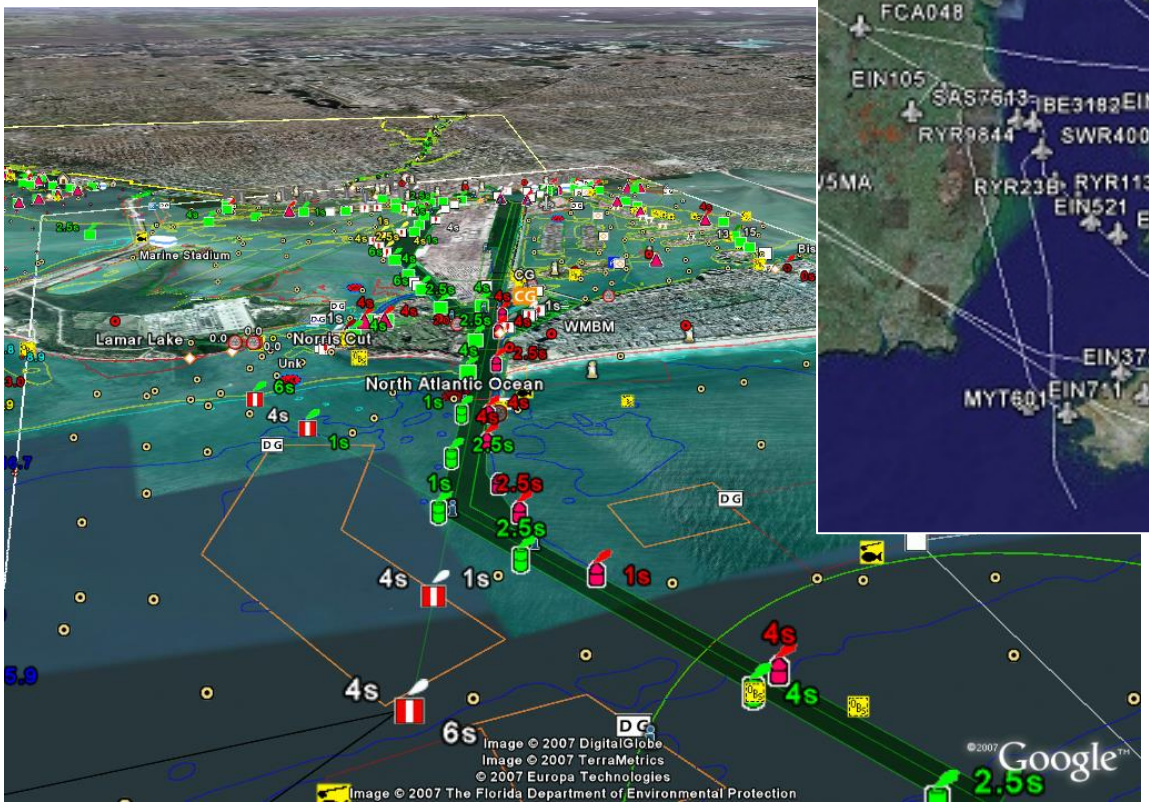
CIO/NII Enabling Net-Centric Operations

# Systems support Missions

**Measurements need to result in data that feeds that support net management, CND, and mission execution.**

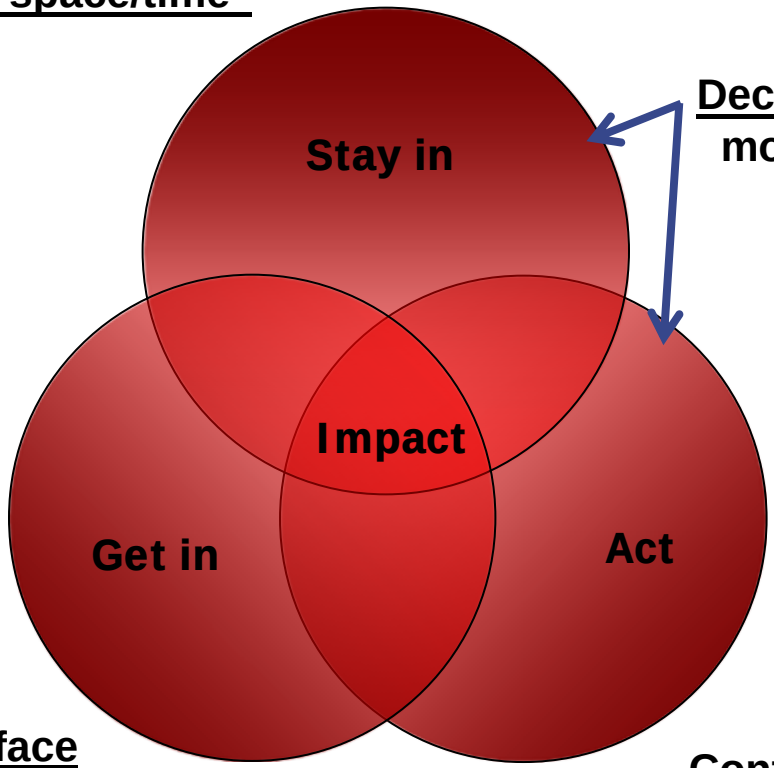
**- Multiple levels of SA to support missions**



# Drive strategies that give us the advantage!

**A trusted environment**
**"Reducing the living-space/time"**



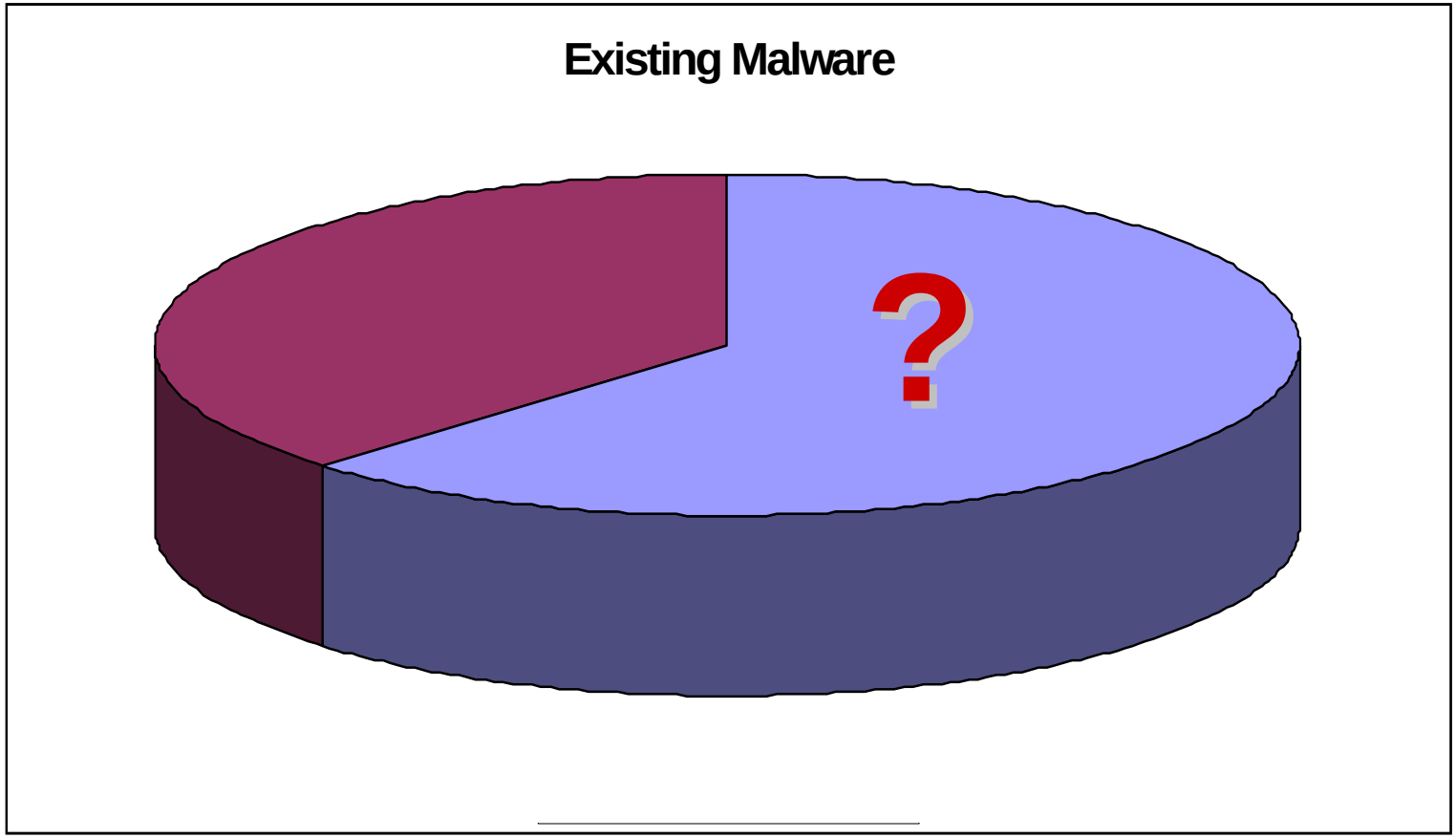

**Dectection -**
**monitoring and analysis**

**Reduce Attack Surface**

**Control of Root Privileges**

Adversary's ability to impact results from success in all three areas – shrinking any of the circles results in a reduced level of impact

# We don't know what we don't know – Protection is preferred, Detection is a must!

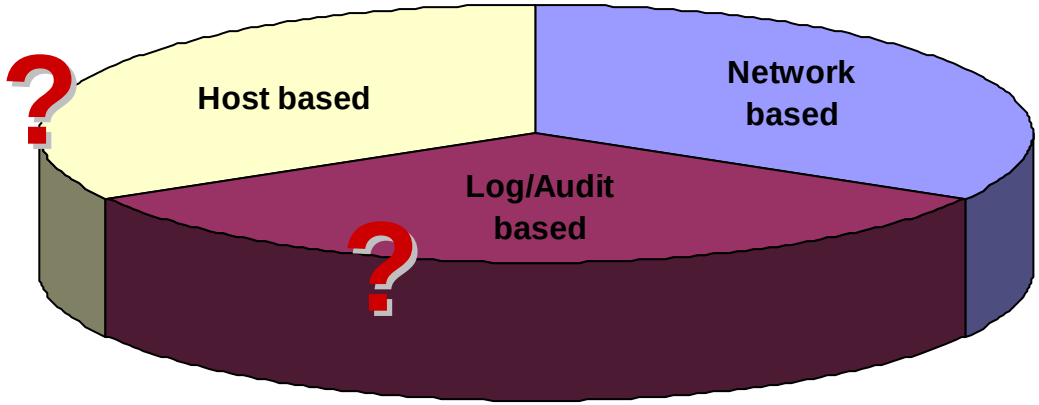



**For every roach that you see…**

# Strategies to increase detection?

**Needs development!**
- Data Strategy – enabling policy and strong configurations

**Heavy focus on network Sensors – currently driving for improvement**
- Communication
- Data Standards

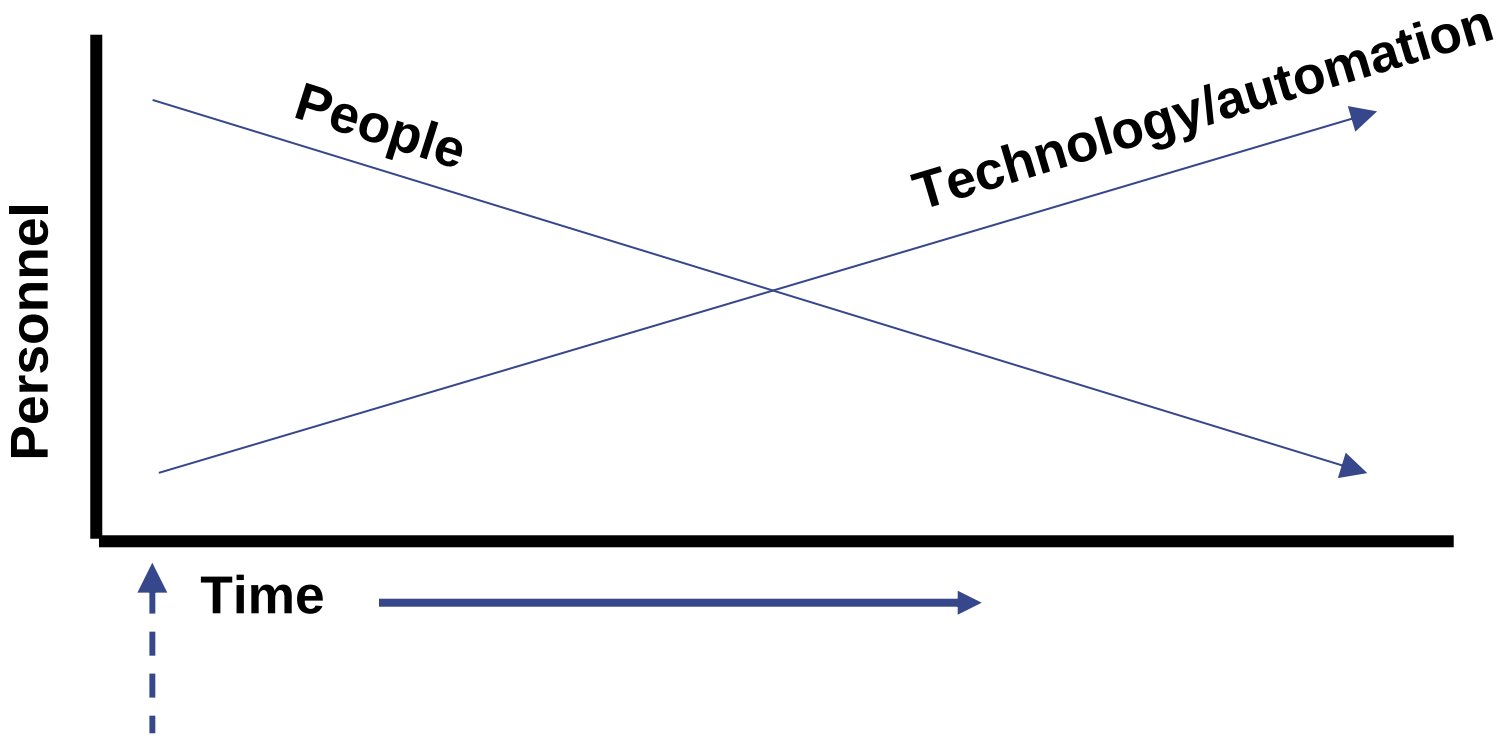



**Measurements and "triggers" for host and log/audit based detection will require much more emphasis**

**Enabling use of logs!**
- Log and Audit data standards
- Secure log servers
- Triggers and indicators?
- Reporting and response

CIO/NII Enabling Net-Centric Operations

# Resources - People vs. technology




CIO/NII
Enabling Net-Centric Operations

# System and Network Hygiene must be improved!

- An issue from the beginning of networked systems…
  - Policies, Directives, Security Guidelines – if implemented would take care of 80% of the problem.

**Why is this problem still here?**

CIO/NII
Enabling Net-Centric Operations

# What clues exist within Event Data?

- Red Teams and audit logs?
- Logging is a requirement – who is looking at them?
- How do we do log and audit records right? How long does it take right now?
- A Huge untapped source of CND Data!
  - We need common Taxonomy, Syntax, Transport and Recommendations – and we need to start doing it right!

CIO/NII
Enabling Net-Centric Operations

# Shift in Strategic Focus

**We need to get to the next level – standards and interoperability are key!**

| FROM | TO |
|---|---|
| • Protect Information | • Ensure Operational Success |
| • Static Pre-Placed Defenses | • Dynamic Network and Information Operations |
| • Proprietary Point Solutions | • Policy-Based Enterprise |
| • People Intensive | • Integrated Services |
| • Fragile Information Technology | • Resilient Cyber Ecosystem |

CIO/NII
Enabling Net-Centric Operations

# Questions?


**Kevin Bingham**
**DoD CND Architect**
**Office of DASD for Information and Identity Assurance**

**michael.bingham@osd.mil**
**703-693-6685**