Developing Systems for Cyber Situational Awareness*

James Okolica, J. Todd McDonald, Gilbert L. Peterson,
Robert F. Mills, and Michael W. Haas

Center for Cyberspace Research
Air Force Institute of Technology
WPAFB, OH

*The views expressed in this article are those of the authors and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the U.S. Government

Overview

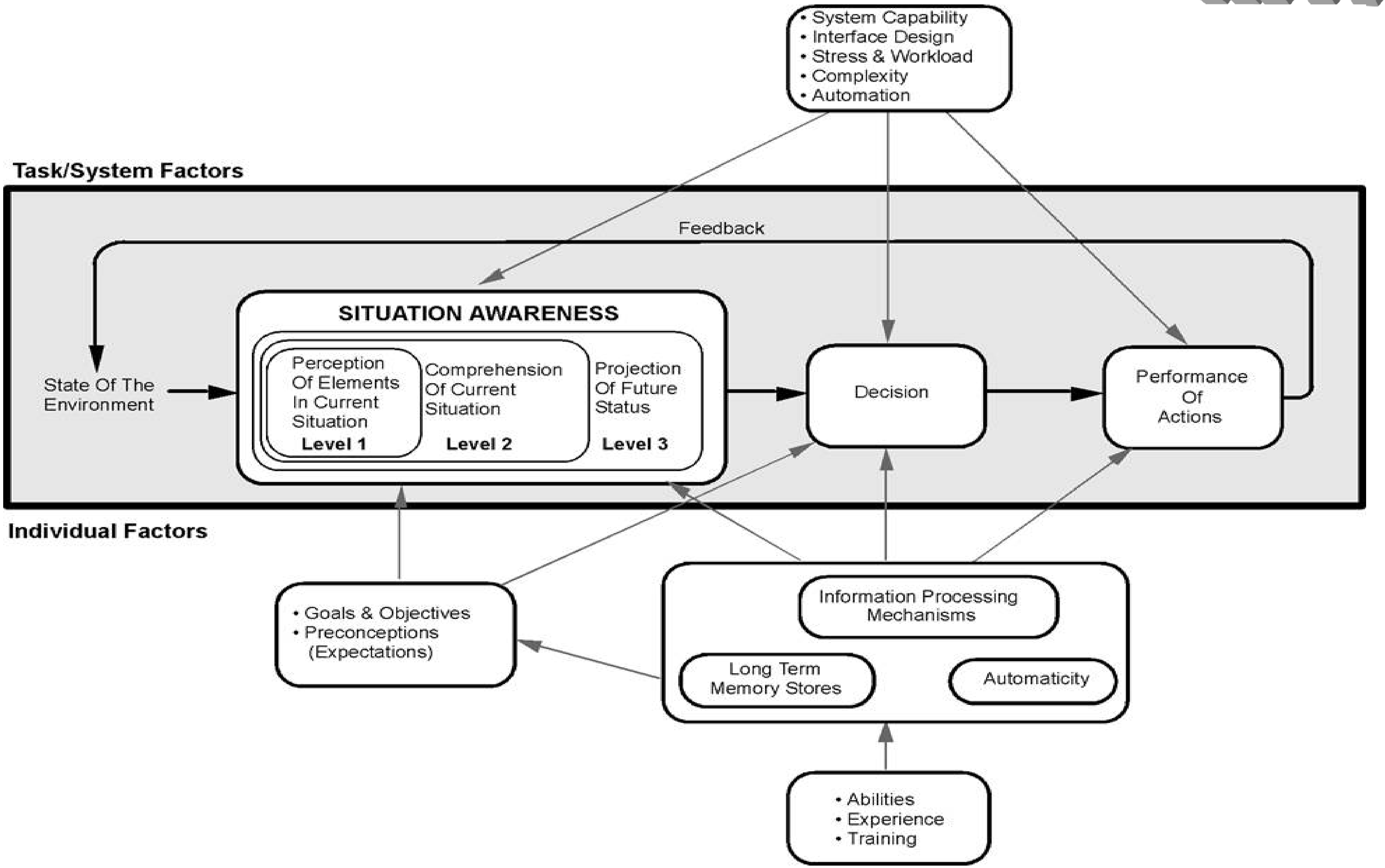
- Defining Cyber Situational Awareness
- The Cyber SA Problem Space
- Developing a Cyber SA System
  - The Perception/ Prediction Loop
  - Understanding the Environment
  - Putting it all together
- Future Work

The Problem

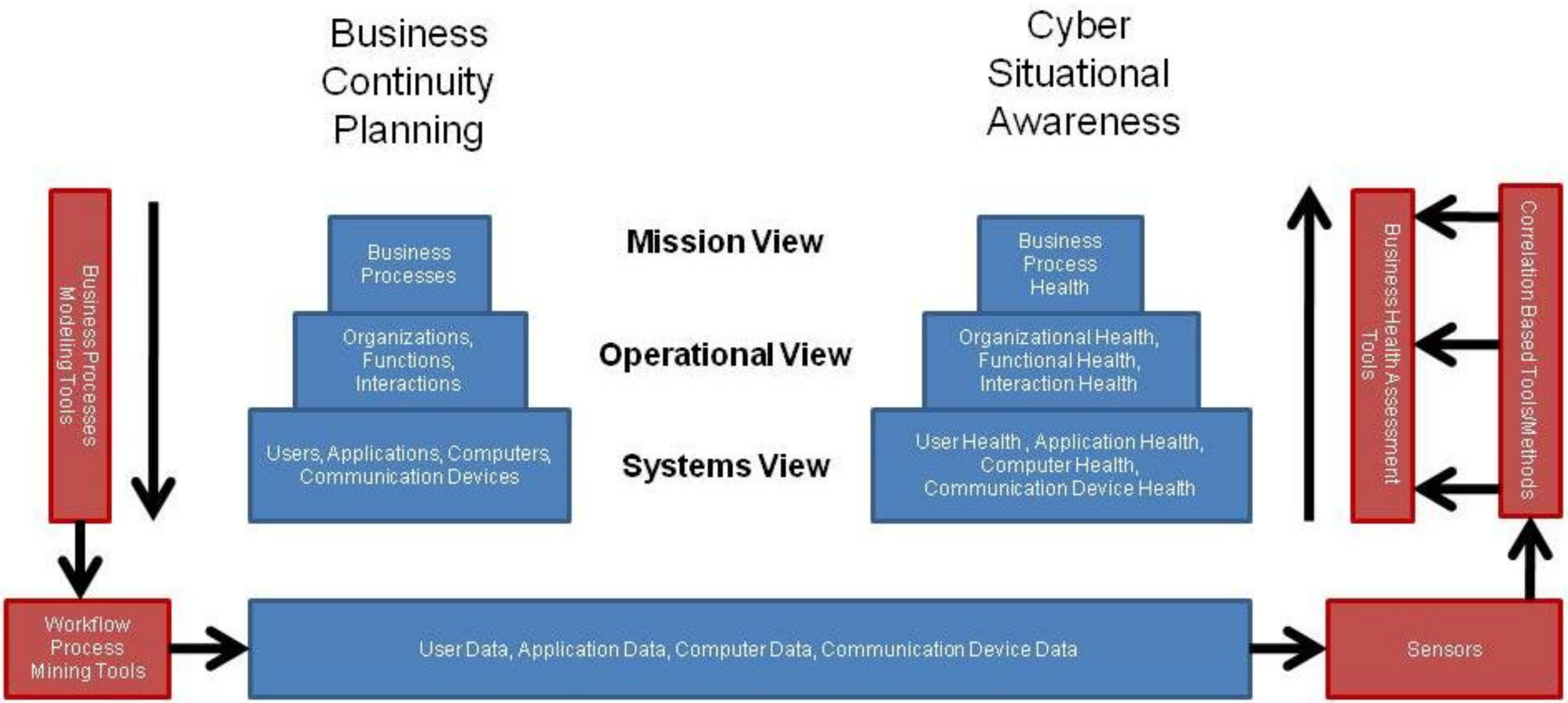
- April 28, 2007 - Distributed denial of service (DDOS) attacks began on a media website in Estonia and would later spread to Estonia’s critical infrastructure including banks, ministries, and police.

- Feb 18, 2001 - Robert Hansen arrested for selling American secrets to Moscow for 22 years

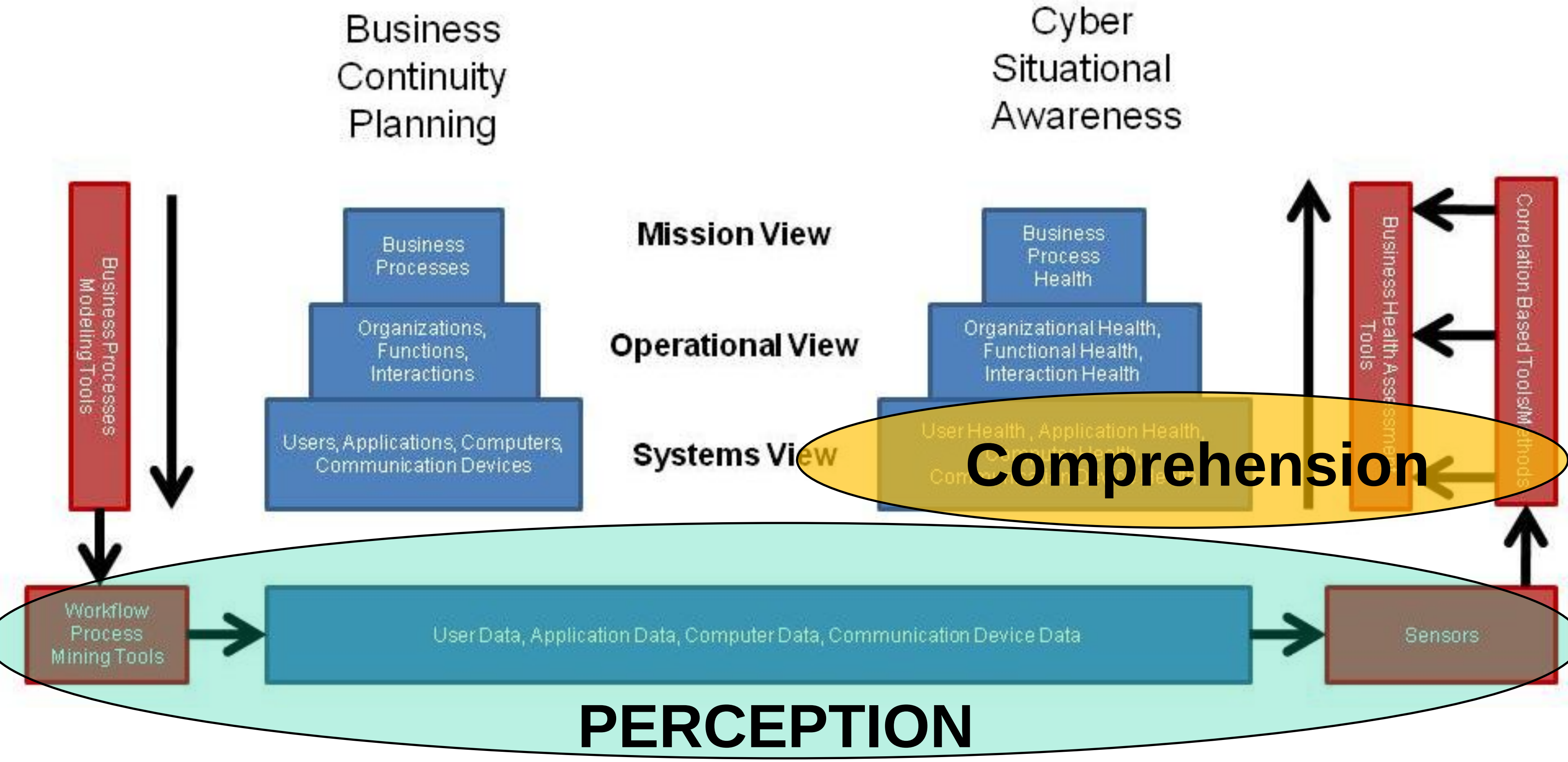
Situational Awareness



Cyber SA


Business Continuity Planning
Cyber Situational Awareness
Business Processes Modeling Tools
Business Processes
Organizations, Functions, Interactions
Users, Applications, Computers, Communication Devices
Mission View
Operational View
Systems View
Business Process Health
Organizational Health, Functional Health, Interaction Health
User Health , Application Health, Computer Health, Communication Device Health
Business Health Assessment Tools
Correlation Based Tools/Methods
Workflow Process Mining Tools
User Data, Application Data, Computer Data, Communication Device Data
Sensors

Cyber SA



Business Continuity Planning

Cyber Situational Awareness

Business Processes Modeling Tools

Business Processes

Organizations, Functions, Interactions

Users, Applications, Computers, Communication Devices

Mission View

Operational View

Systems View

Business Process Health

Organizational Health, Functional Health, Interaction Health

User Health , Application Health, Computer Health, Communication Device Health

Business Health Assessment Tools

Correlation Based Tools/Methods

Comprehension

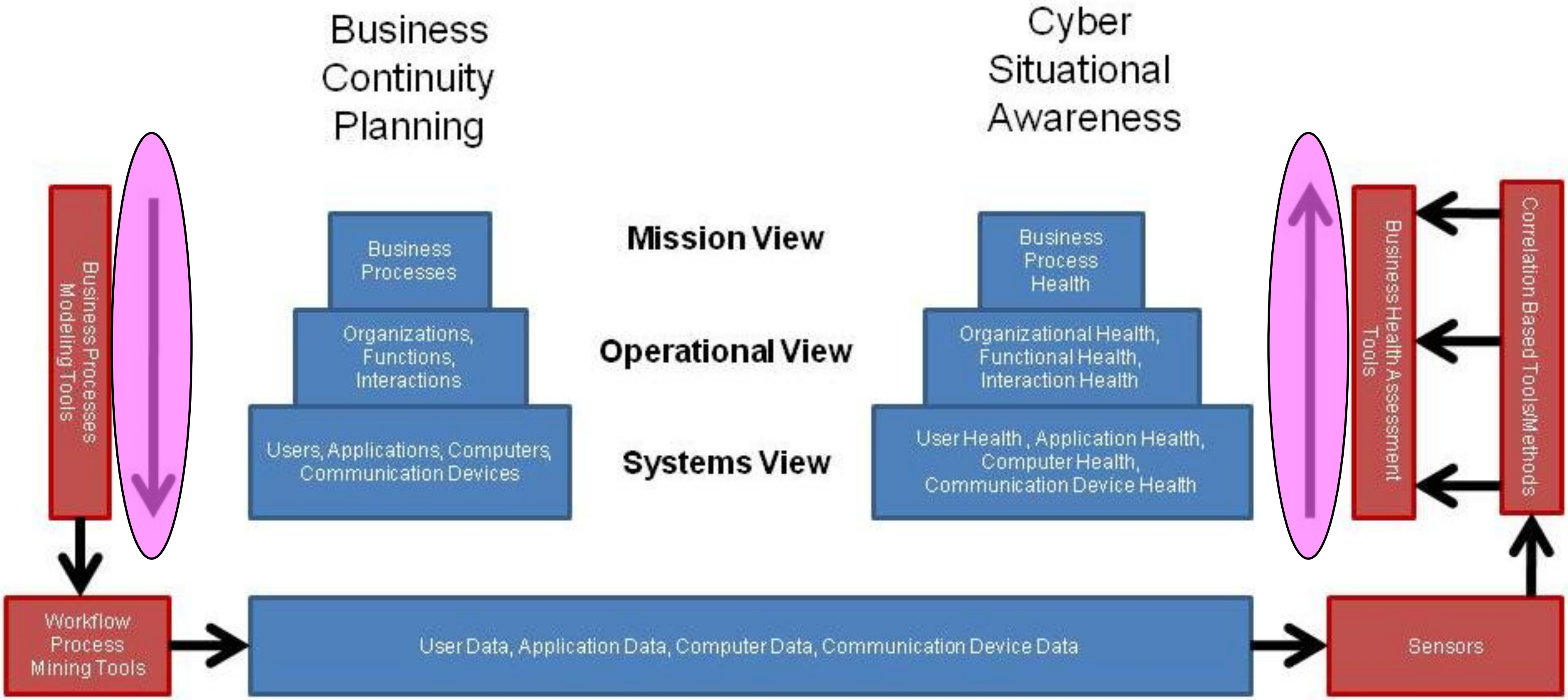
Workflow Process Mining Tools

User Data, Application Data, Computer Data, Communication Device Data

Sensors

PERCEPTION

Cyber SA

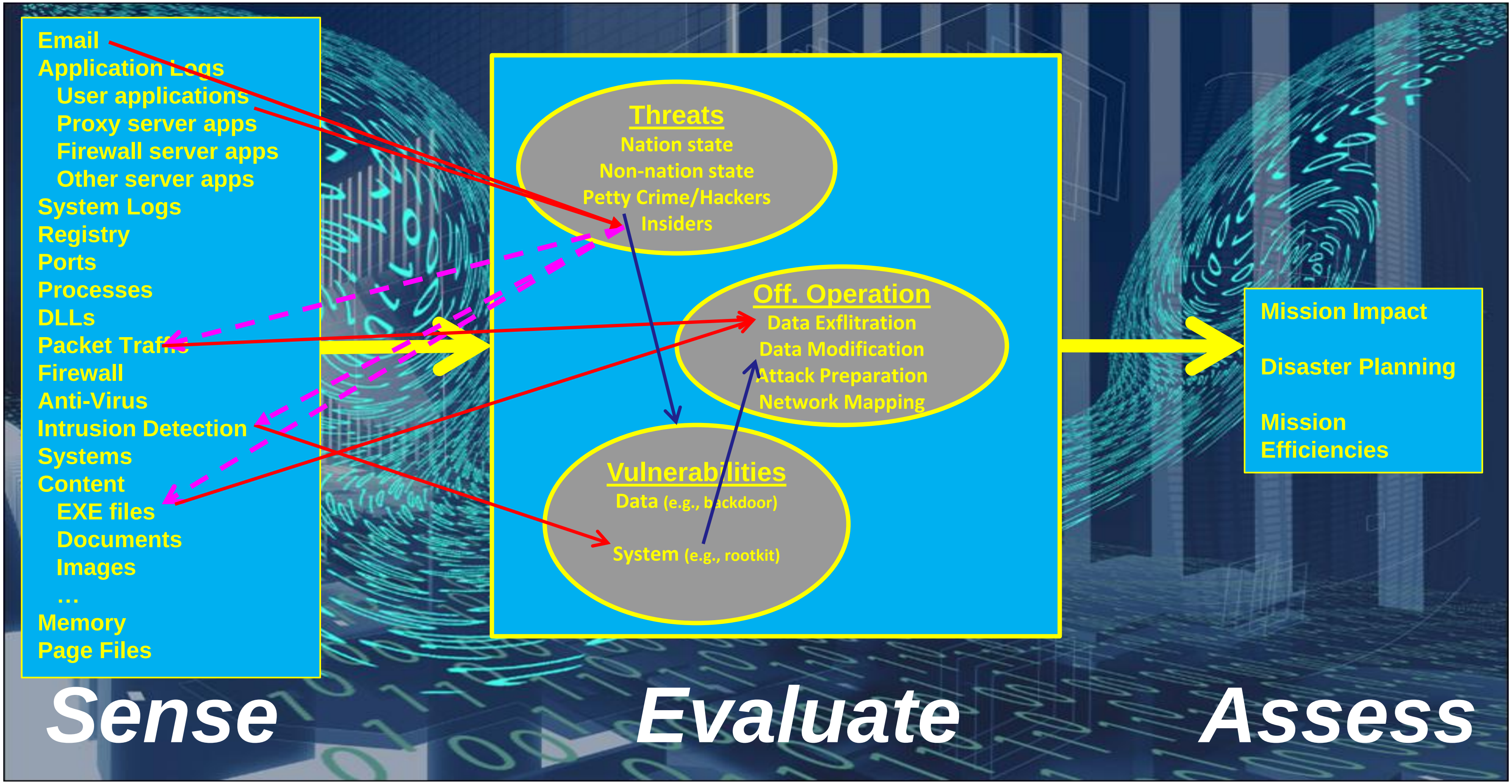

Business Continuity Planning
Cyber Situational Awareness
Business Processes Modeling Tools
Business Processes
Organizations, Functions, Interactions
Users, Applications, Computers, Communication Devices
Mission View
Operational View
Systems View
Business Process Health
Organizational Health, Functional Health, Interaction Health
User Health , Application Health, Computer Health, Communication Device Health
Business Health Assessment Tools
Correlation Based Tools/Methods
Workflow Process Mining Tools
User Data, Application Data, Computer Data, Communication Device Data
Sensors

Insider Threat Cyber SA

Individual Devices

Data Environment

Business/Mission Environment



Email
Application Logs
User applications
Proxy server apps
Firewall server apps
Other server apps
System Logs
Registry
Ports
Processes
DLLs
Packet Traffic
Firewall
Anti-Virus
Intrusion Detection Systems
Content
EXE files
Documents
Images
…
Memory
Page Files

Threats
Nation state
Non-nation state
Petty Crime/Hackers
Insiders

Off. Operation
Data Exflitration
Data Modification
Attack Preparation
Network Mapping

Vulnerabilities
Data (e.g., backdoor)
System (e.g., rootkit)

Mission Impact

Disaster Planning

Mission Efficiencies

Sense

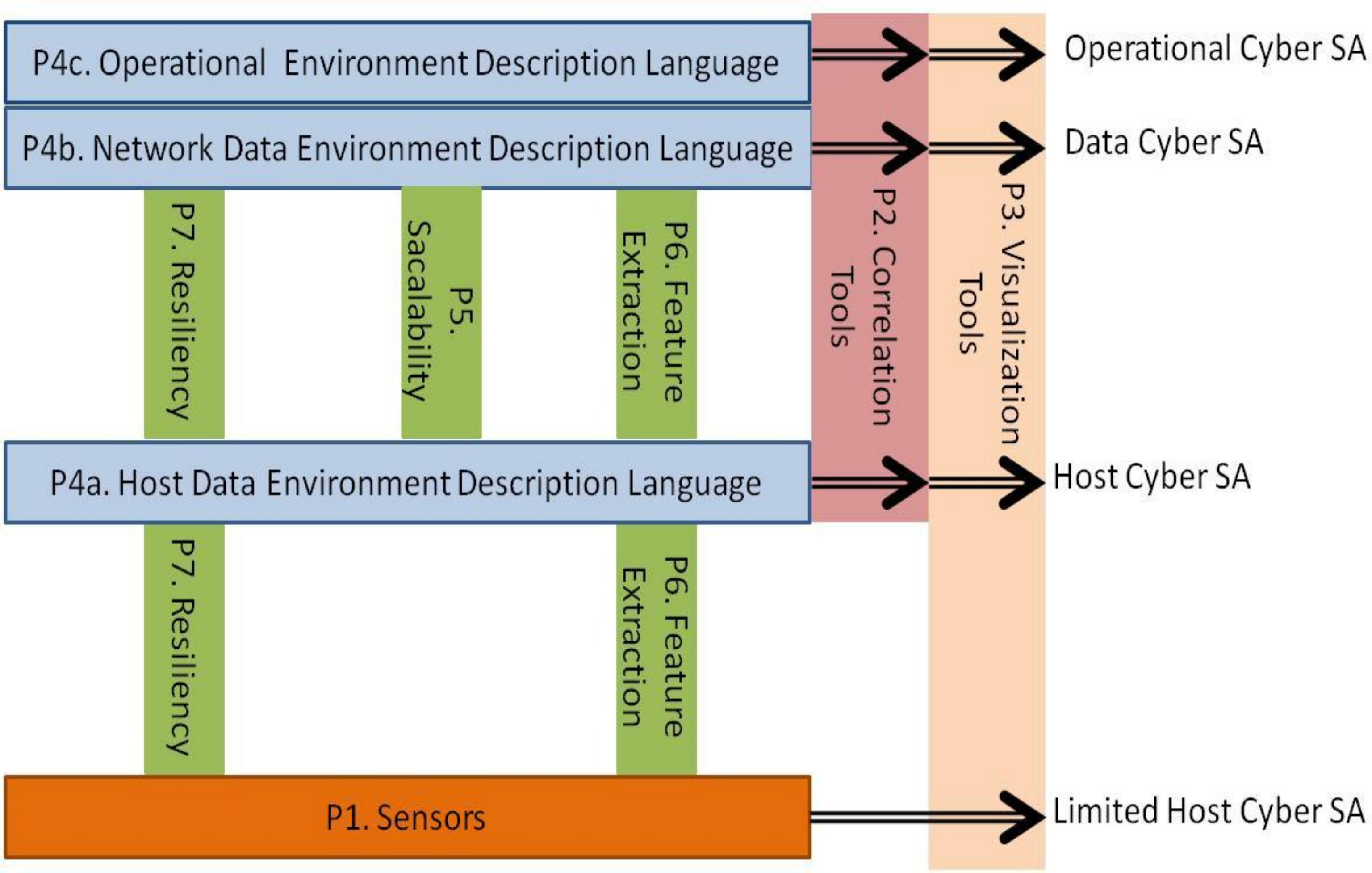
Evaluate

Assess

Perception/ Prediction Loop

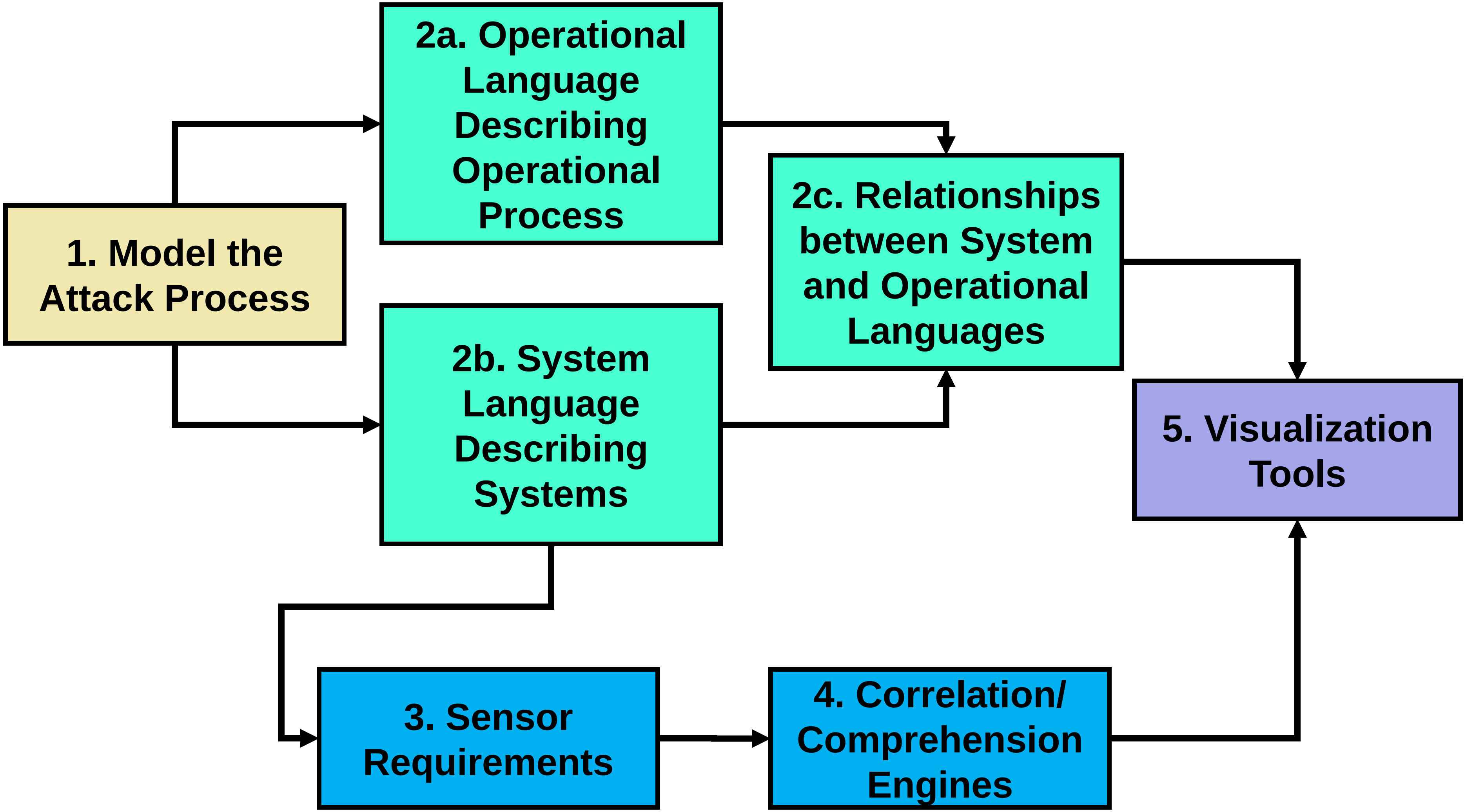
- Model the Attack Process
- Extract sensor requirements for each step in the process
- Categorize sensors as
  - Distant Early Warning (DEW) line sensors – with minimal footprint to host systems, provide a high confidence of anomaly detection – lots of false positives
  - Focused sensors – more intrusive, processor intensive sensors that are tailored to detecting much more specific attacks
- Develop and deploy sensors
- Activate DEW line sensors
- When DEW line is tripped, activate the focused sensors

Multi-level Comprehension



Developing a Cyber SA System

Develop America's Airmen Today ... for Tomorrow


1. Model the Attack Process
2a. Operational Language Describing Operational Process
2b. System Language Describing Systems
2c. Relationships between System and Operational Languages
3. Sensor Requirements
4. Correlation/ Comprehension Engines
5. Visualization Tools

Next Steps

- Develop Cyber Attack Models for multiple types of attacks
- Extract requirements and develop sensors

What about BPM?

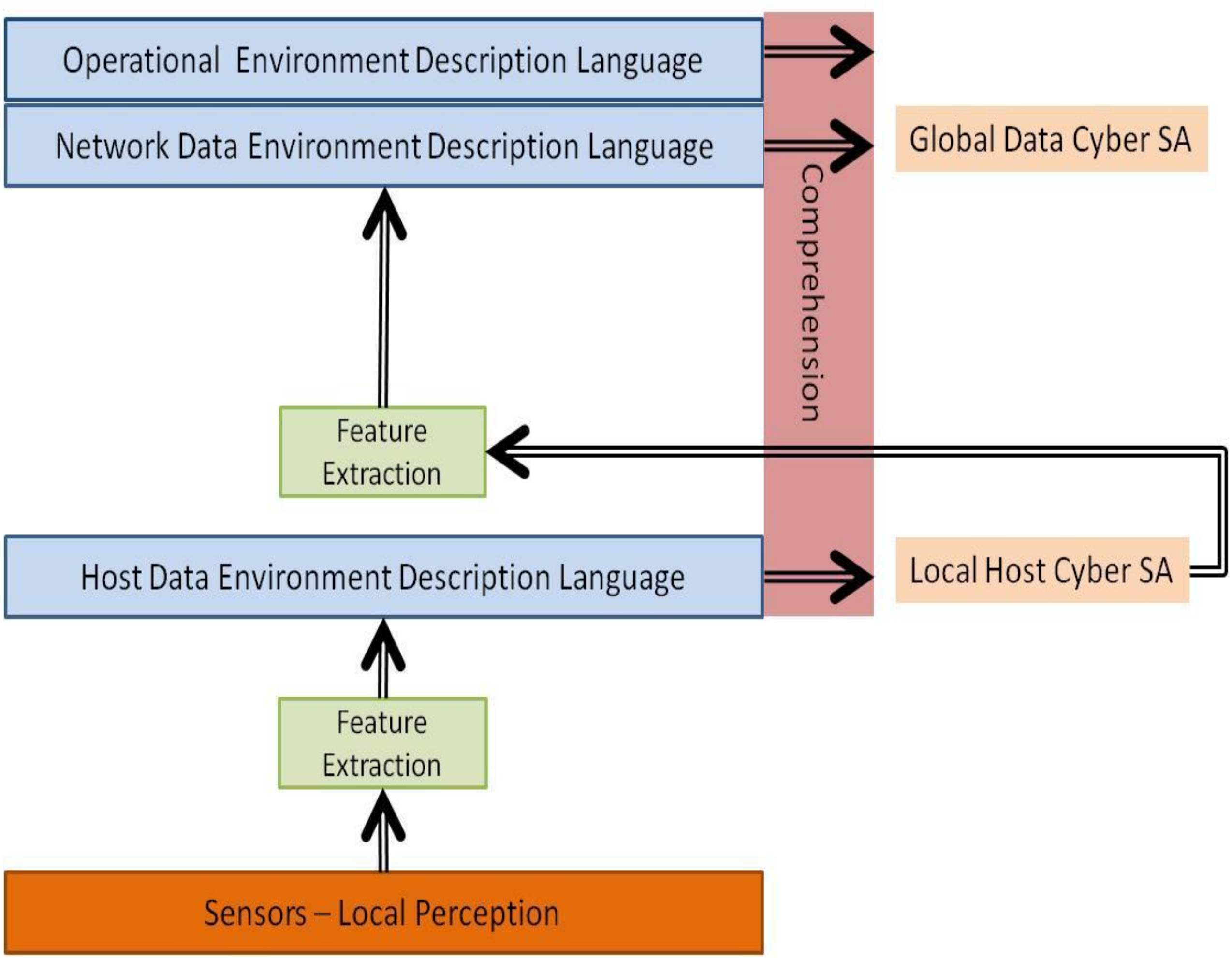
- Organizations design may oppose BPM - Stature by how large/ how much money
- Wisdom of putting BPM on a networked computer
  - Cyber SA in place to secure network
  - However, Cyber SA depends on BPM for mission impact
  - BPM defines critical nodes and single points of failure
  - Tradeoff
    - Increased responsiveness & improved management situational awareness
    - Greater vulnerability to precision attack

Questions

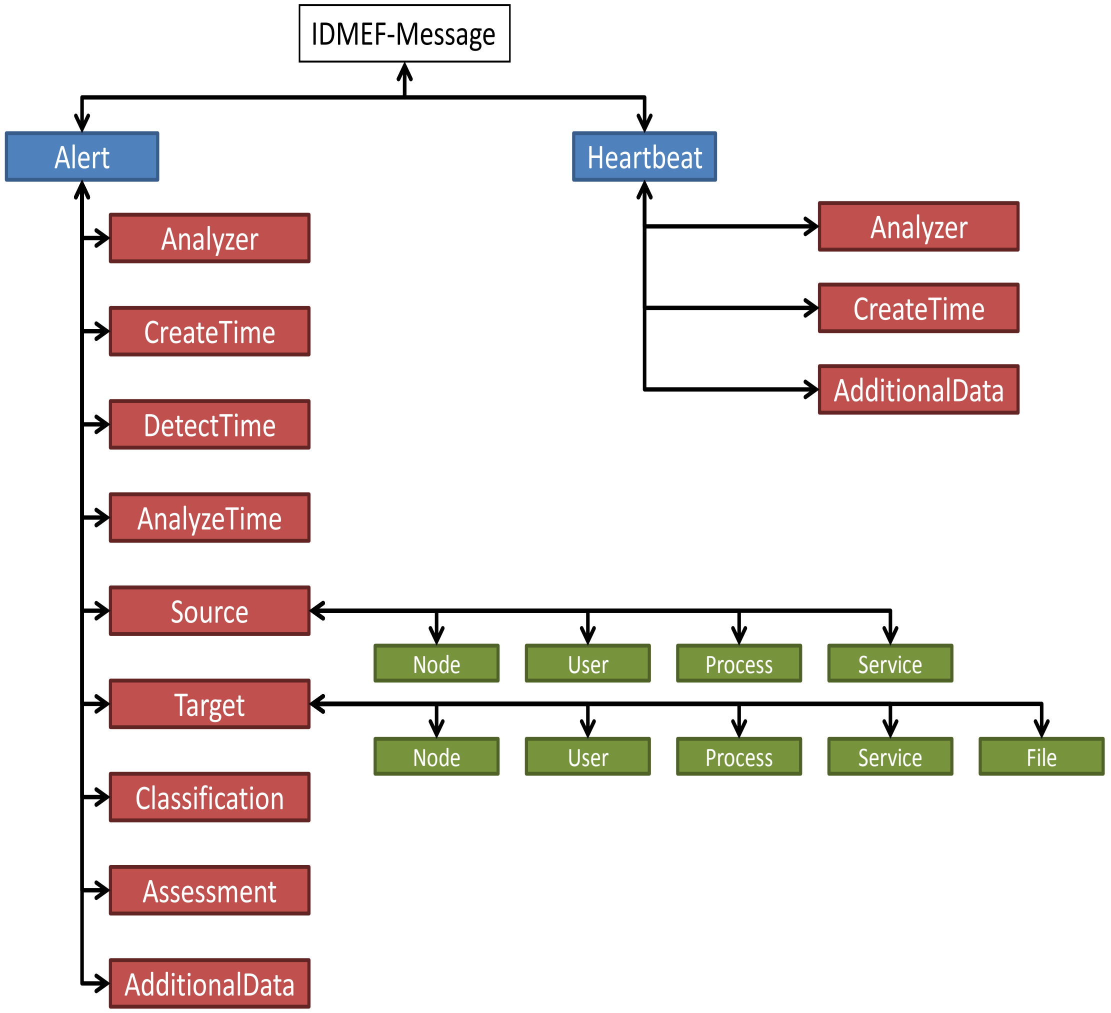
?

Backup Slides

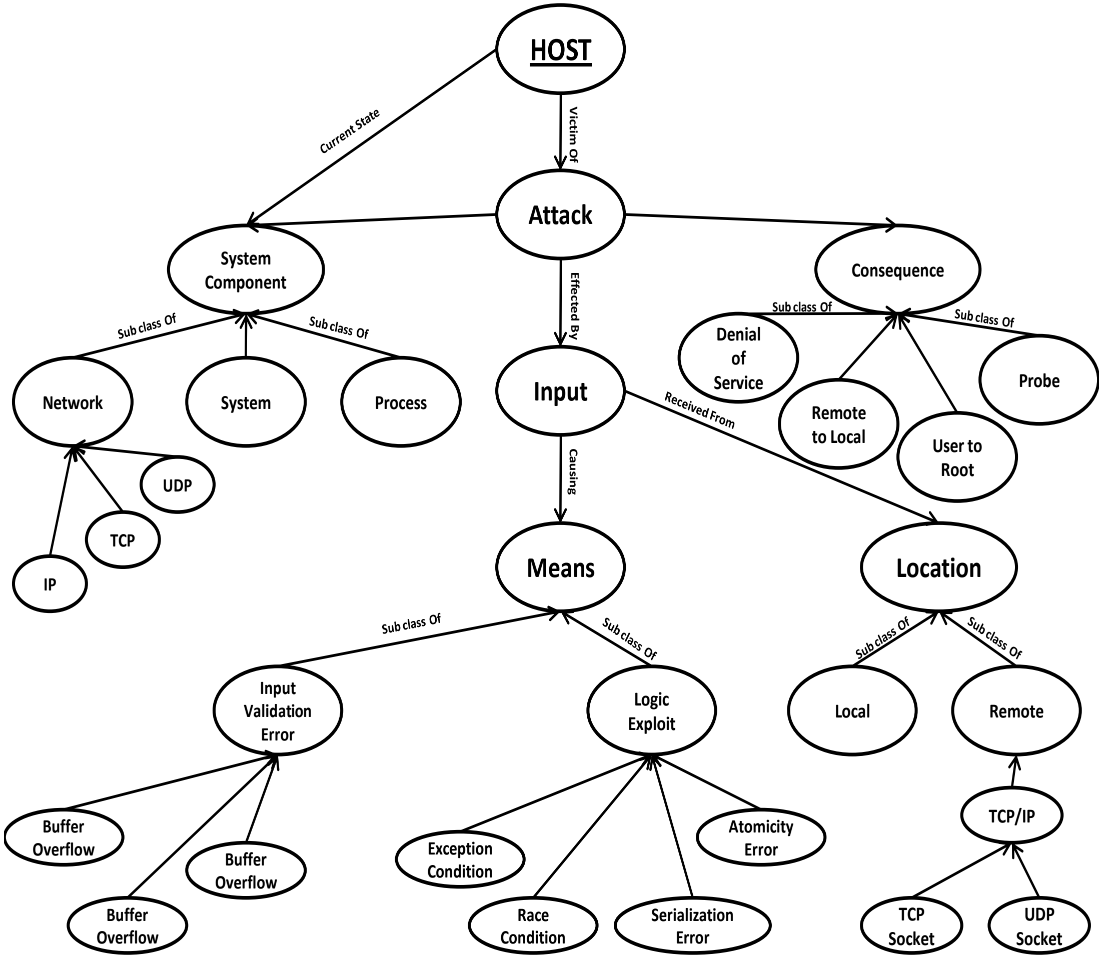
Cyber SA Environment


Operational Environment Description Language
Network Data Environment Description Language
Global Data Cyber SA
Comprehension
Feature Extraction
Host Data Environment Description Language
Local Host Cyber SA
Feature Extraction
Sensors – Local Perception

IDMEF Data Model



Target Centric Ontology



Information Relativity

- Consider the data object “mission”
- Does an object mean different things at different levels?
- Does an object mean different things within a level depending on the producer/consumer of the object?