



# ***INNOVATIVE SOLUTIONS FOR THE CYBER WARFIGHTER***

*Integrity - Service - Excellence*



## **The Need for Real Time Cyber Incident Mission Impact Assessment**



**Michael R. Grimaila, *Senior Member, IEEE***  
**PhD, CISM, CISSP, NSA IAM/IEM**  
Center for Cyberspace Research  
Air Force Institute of Technology

**IEEE Intelligence and Security Informatics  
Conference 2009**

**Richardson, Texas**  
**11 June 2009**

**Sponsor:**  
**Air Force Research Laboratory (AFRL/RHX/711th HPW)**

**UNCLASSIFIED: Distribution A: Approved for public release**



# Disclaimer

---



*The views expressed in this presentation are my own and do not reflect the official policy or position of the United States Air Force, the Department of Defense, or the United States Government*

---



# Overview

---



- **Research Motivation**
  - **Background**
  - **Problems Identified**
  - **Towards a Cyber Incident Mission Impact Assessment (CIMIA) Capability**
  - **Conclusions and Future Work**
-



# A Hypothetical Scenario?

---



- A coalition partner is provided connectivity to a US military network for information sharing
  - A breach of a coalition partners system occurs
  - The breach enables an adversary to access a server which contains multiple databases, including one that contains planned convoy routes and schedules
  - Some time later, the breach is detected and stopped
  - The IRT works with the system custodians to identify and notify the information owners and (ideally) all system users
  - The process takes days to complete...
  - The convoy unit is contacted, but the POC has only been in their new position less than a week
  - As a result, the convoy commander is not notified...
-



# The Consequences



الجيش الإسلامي في العراق / تدمير مدرعة للجيش الأمريكي المحتل في منطقة التاجي



# Sun Tzu

---



*“Know your enemy and know yourself  
and you can fight a hundred battles  
without disaster.”*

---



# Background

---



- **Virtually every organization is dependent upon information accessed/stored/processed in cyberspace**
  - **Despite our best efforts at developing defensive capabilities, cyber incidents are inevitable**
  - **Cyber dependence introduces significant risk to both cyber operations and real-world operations**
  - **Commanders need accurate, timely, and relevant damage assessment in terms of their own mission**
  - **This is not a new development (RAND Report, 1995)**
  - **Today we measure success as maintaining awareness of what systems we have (e.g., hardware, software, configuration, patches, antivirus, HIDS)**
-



# Prior Research

---



- **Ware Report (1970) – DoD mission relies on computing systems**
  - **RAND Report (1995) – The Day After Exercises**
  - **Lala and Panda (2001) – Database damage assessment**
  - **Thiem (2005) – Lack of standardized AF damage assessment methodologies**
  - **Stanley (2005) – Mission impact analysis of communication link state availability**
  - **Wong-Jiru (2006) – Net centric operations model for holistic view of mission dependencies between entities**
  - **Shaw (2007) – Model of network outages in CAOC**
  - **Fortson (2007) – Proposed a defensive Cyber Damage Assessment (CDA-D) methodology**
  - **Hellesen (2008) – Information valuation schema**
  - **Sorrels (2008) – System architecture for CIMIA**
-



# Key Problems Identified

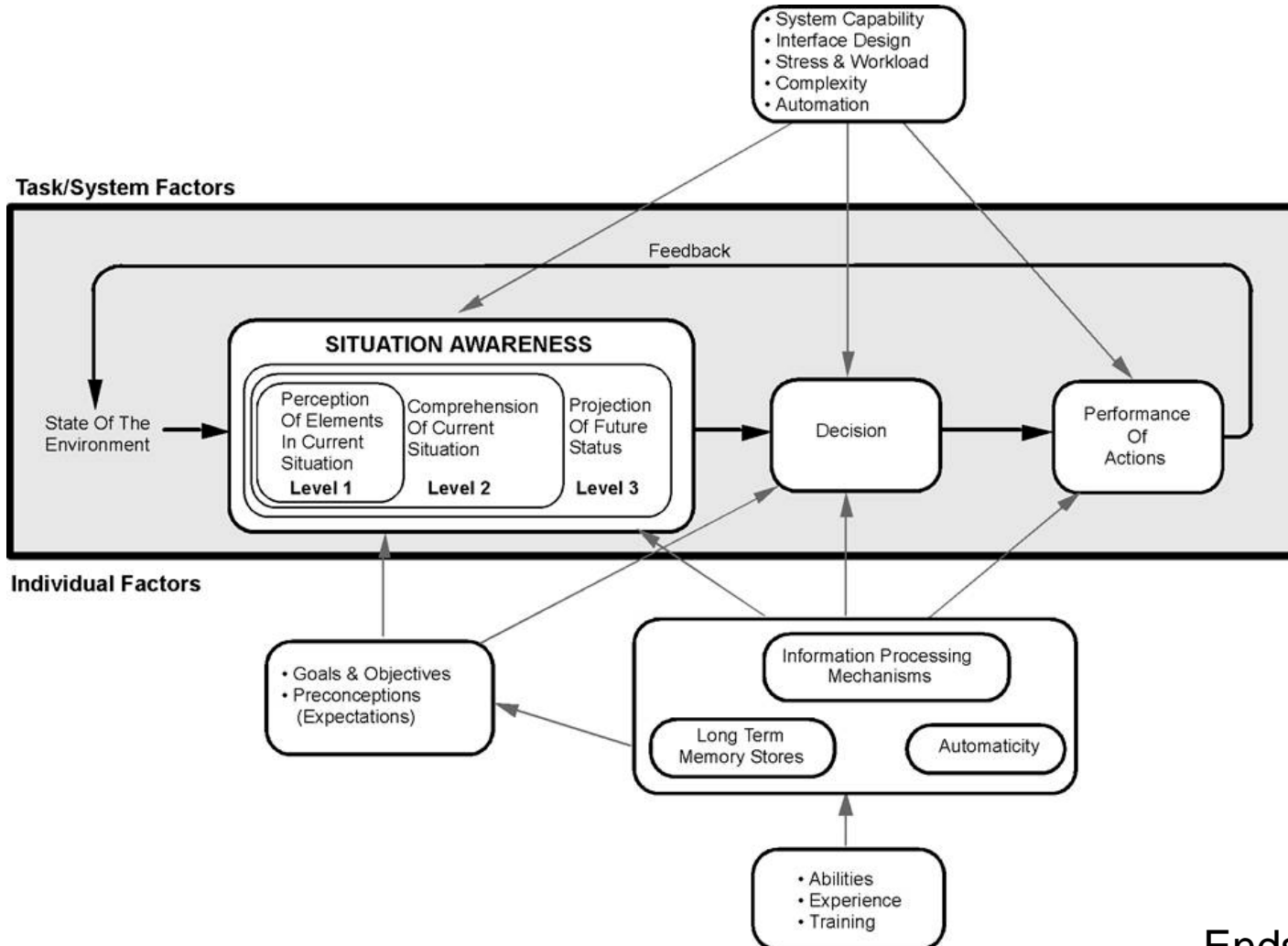
---



- A fixation on system and infrastructure protection
  - Lack of a standardized risk assessment process
  - Lack of documentation explicitly identifying information assets and their mission value
  - Lack of timely and relevant notification of ALL information consumers following cyber incidents
  - Lack of an appreciation for potential impacts
  - Lack of accountability and after action follow-up
  - The nature of federated organizational structure
  - Lack of knowledge continuity
  - We don't collect, document, maintain, refine, disseminate, and exploit knowledge of mission-to-information dependencies effectively!
-



# Situational Awareness



Endsley, 2007

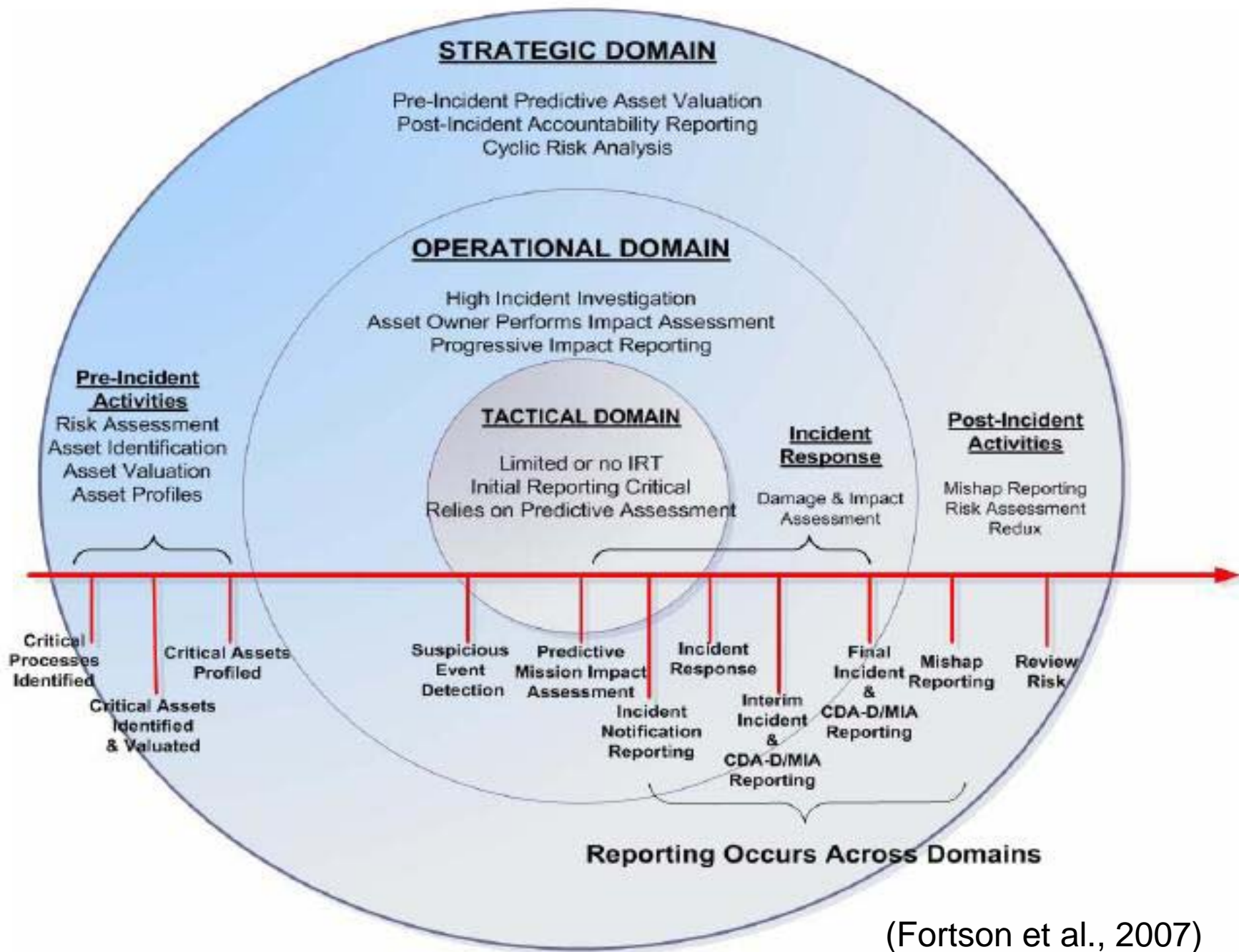


# Risk Assessment

---



- Risk Assessment requires the identification and documentation of critical organizational resources
  - Criticality is determined by how a given resource supports the organizational mission
  - The valuation of any resource is:
    - Frame of reference dependent
    - Temporally dependent upon the mission(s)
    - Inherently subjective ← SMEs needed
  - Risk to a resource is an expected loss:
    - $(\text{Threats} \cap \text{Vulnerabilities}) * \text{Probability} * \text{Loss}$
  - Allows for a racking and stacking of the risks
-



(Fortson et al., 2007)



# Impediments to Risk Assessment

---



- Labor intensive
  - Time consuming
  - Must periodically be revisited (maintenance)
  - Several different organizations may access and depend upon a resource (hard to estimate value)
  - Status Quo
  - Unwanted accountability
  - Knowledgeable personnel must value resources
  - Security aspects of critical asset identification
- \* In the DoD we instead rely on the National Security Classification process and the Certification & Accreditation of systems (DIACAP) as our RA
-



# Albert Einstein

---



*“In the middle of difficulty lies opportunity.”*

---



# Cyber Incident Mission Impact Assessment (CIMIA) Project

---



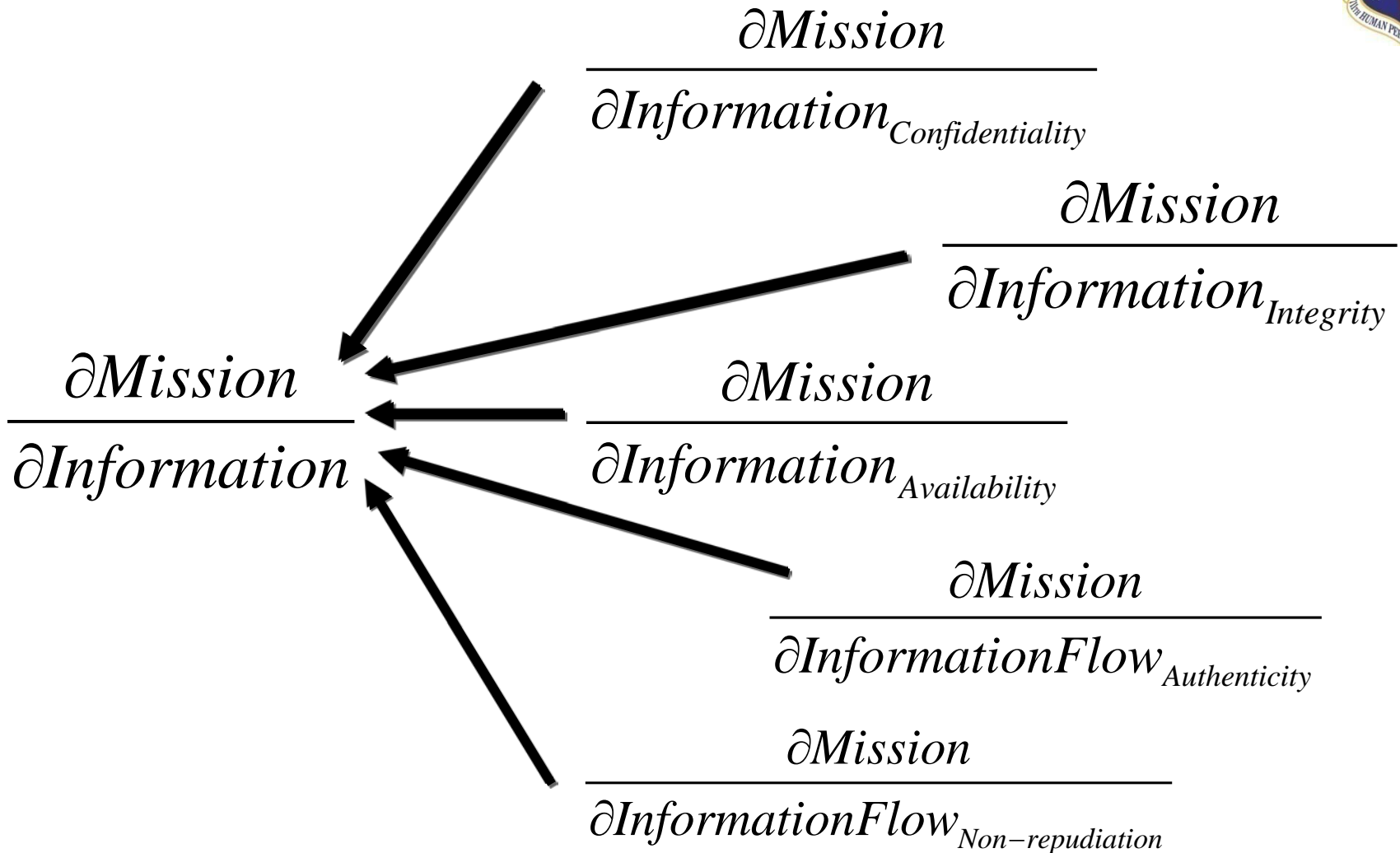
- Develop a structured process to provide decision makers with context specific, real-time situational awareness of the status of critical information resources
- Provide timely and relevant notification of estimated mission impact following an incident, from the time it is declared, until the incident is fully remediated

**\*\* Requires an Explicit Mission Representation \*\***

- Mission Impact not only as a function of Availability:
    - Confidentiality
    - Integrity
    - Authenticity
    - Non-Repudiation
-



# Mission-Information Impact Assessment





# CIMIA Objectives



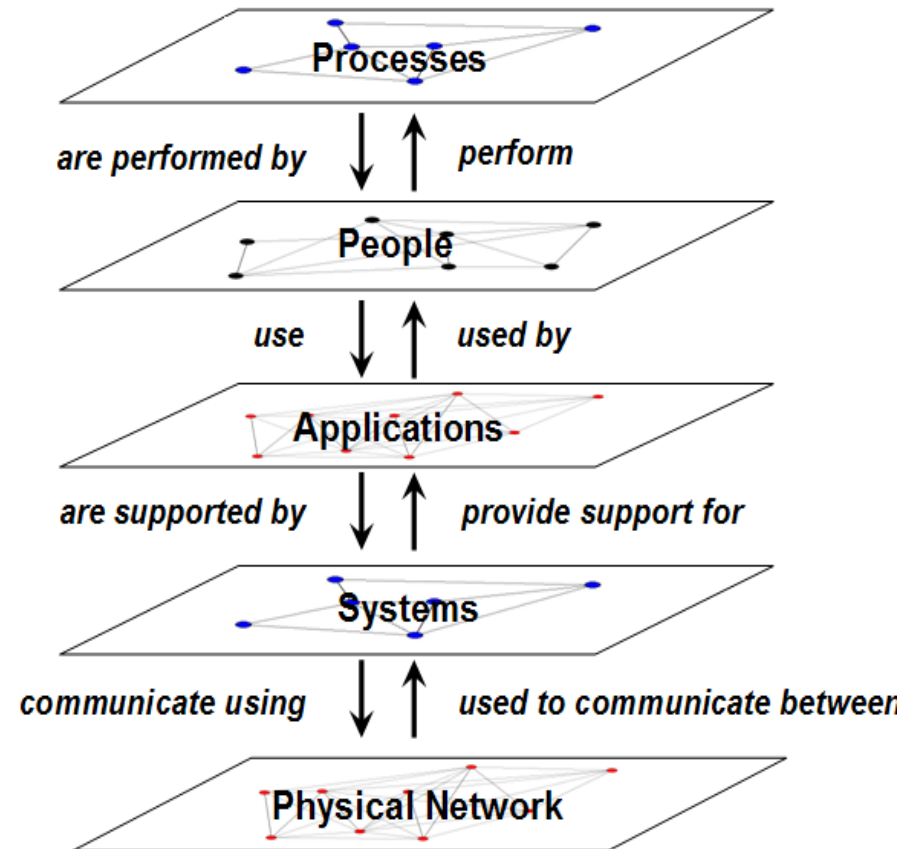
- Mapping of “mission” to required information assets
- Secure, automated notification of all downstream information consumers when an incident occurs
- Mission impact assessment from incident declaration (estimated) through remediation (actual)
- Explicit accounting for uncertainty over time
- Global tracking of the “state” of information
- Mission representation and visualization
- Temporal mission information valuation
  - Learn historical mission patterns
- Enforce:
  - Accountability / Documentation / Secrecy



# Mission Mapping Abstractions



- How to best map mission to underlying information resource dependencies?
- How to represent the “value” provided by each intermediate resource?
- What is necessary and feasible to collect and maintain in a mapping?
- How to insure an adversary cannot access and exploit this information?





# CIMIA Elements

---



- **Information asset identification**
  - **Information asset valuation**
    - **How do we capture information valuation?**
  - **Mission-Information mapping**
    - **How do we capture and update mission-information dependencies as they change?**
  - **Tracking information consumers**
  - **Secure notification and reporting**
    - **Mission impact estimation from initial estimation (high uncertainty) to incident remediation (low uncertainty)**
  - **Knowledge retention and continuity**
-



# Information is THE Asset

---



- Information is data communicated, processed, stored, retrieved, and disseminated in cyberspace by human beings
  - Information supports real world mission operations
  - Each individual has a different valuation “lens” through which they view information assets
  - We must account for the value of information through its whole lifecycle
  - The value of information changes over time as the mission evolves
  - We must track the “state” of information
  - Who is dependent upon a given information asset?
-



# Information Asset

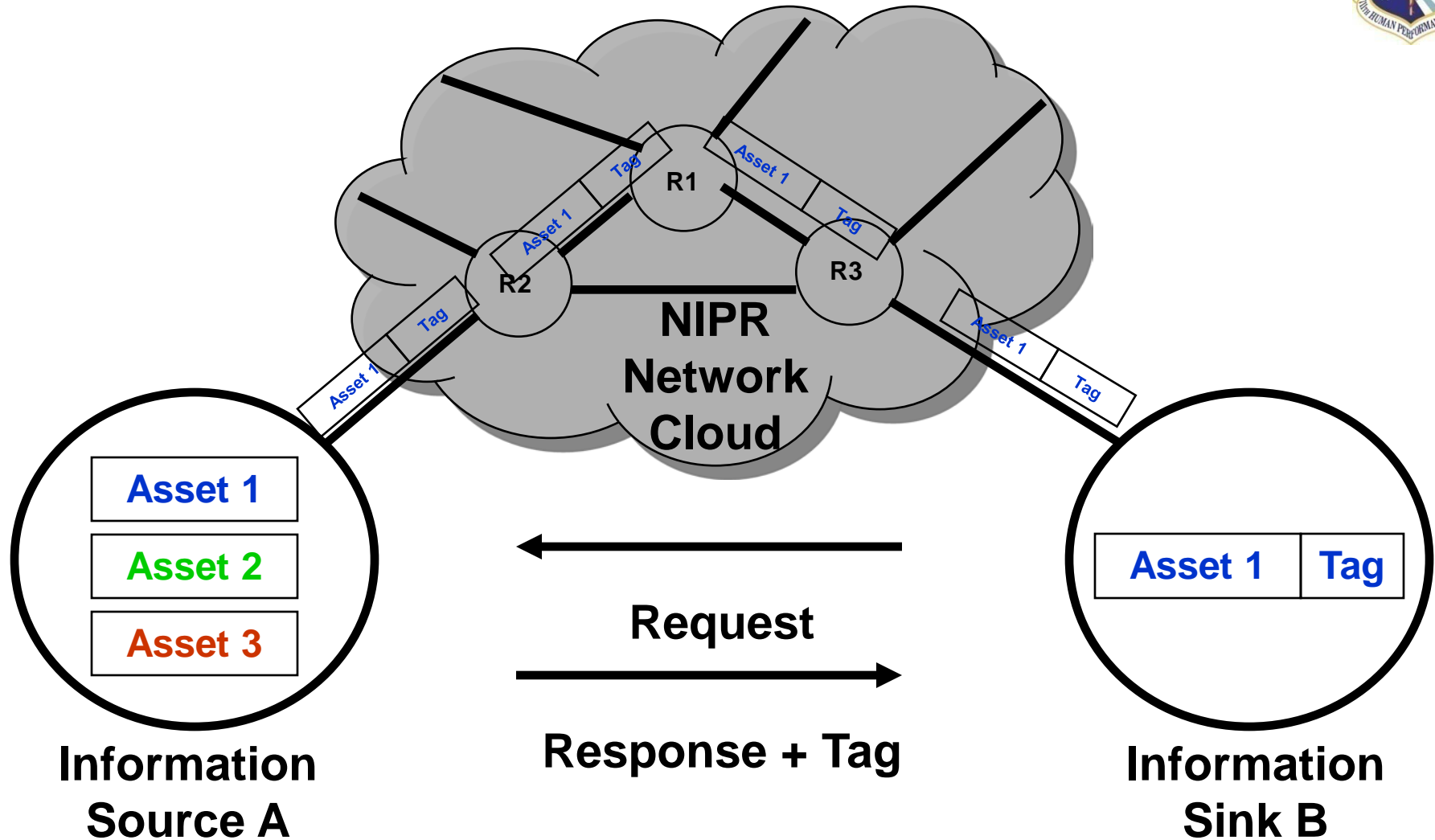
---



- **A specific grouping of data which provides value**
  - **The granularity is user definable**
    - **Coarse: All information contained in a system**
    - **Fine: A specific attribute within a specific record within a specific database within a system**
  - **Multiple information assets reside within the same information container / flow through network**
  - **Each information asset must be uniquely identifiable across the enterprise**
  - **Multiple information assets may be repackaged with other information, creating a new information asset (e.g., intelligence reports)**
  - **How can we manage / track our information assets?**
-



# Information Asset Tagging Source / Sink Architecture





# Information Asset Tags

---



- Each information asset has an enterprise-wide key (“tag”) which is used to uniquely identify it
  - The “tag” is encrypted to confuse snooping
  - The “tag” is a pointer into a database which contains metadata about the information asset
  - When an information asset is moved, the tag moves
  - Tagging of information assets enables the tracking of the assets from the source (provider), through the infrastructure elements, to the sink (consumer)
    - Accountability can be enforced
    - Network traffic can be prioritized
    - Mission specific patterns can be identified
-



# Tag Insertion



- Tags are “intelligently” inserted into the network data stream at the source by a defined policy:
  - One time for a given requestor
  - After a defined time interval has passed
  - When a change in the asset occurs
- Very low overhead impact
- Tag may be inserted in multiple ways (e.g., unused bits, IPV6 Flow Label, encoded into data, stego)
- The tag itself does NOT contain any information about the information asset
- The tag is an encrypted using symmetric encryption
- The tag encryption changes daily using an automated process that is seeded monthly



# Information Asset Database

---



- **A database containing information about the given information asset from the owners perspective:**
    - Key “Tag”
    - Owner
    - Producer
    - Provider
    - Pedigree
    - Age
    - Comments
    - Composite elements
    - Confidentiality Sensitivity
    - Integrity Sensitivity
    - Availability Sensitivity
    - Rated Criticality
    - Derived Criticality
    - Last update
  - **Maintained by a central authority (e.g., JTF-GNO)**
  - **Global database located in a higher classification network only accessible by authorized entities**
-



# Fictional Information Asset Database



Tag	Owner	Producer	Age	Owner Criticality	Contains	SA_LABEL
7FD3BA30	AFIOC	33rd IOS	Daily	Very High	23A9D3D7, DD3100AC	TS-SCI/HCS
B723AA29	67th NWW	GREEN	10 June 2008	High	<NULL>	S/BELL
23A9D3D7	NASIC	SMAI	Daily	Very High	<NULL>	TS-SCI/TK
DD3100AC	NSA	GROUP 4	Weekly	High	<NULL>	TS-SCI/G

Note: Not all fields are shown for brevity



# Linking Mission Relevance to the Information Asset



Mission Process Supported

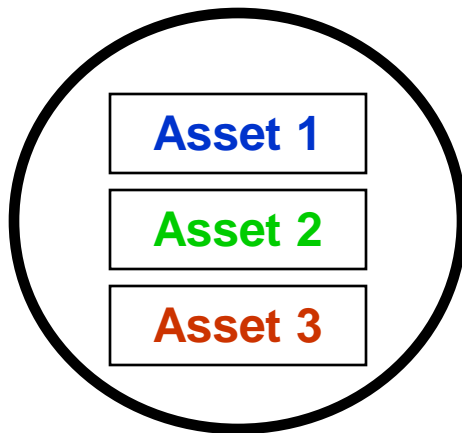
Mission Importance

105811JUN09	B	Bob

105811JUN09	A	Tag

 + 

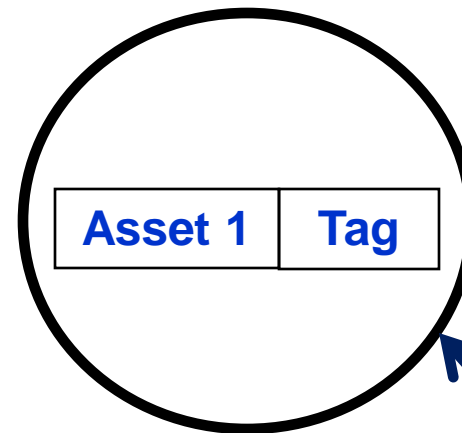
Weather	5



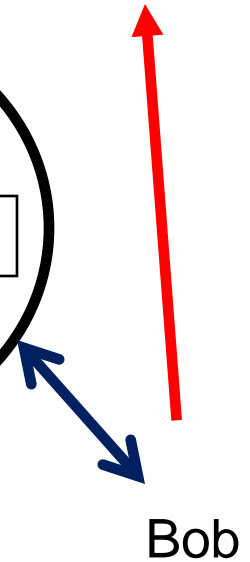
Information Source A



Response + Tag



Information Sink B



Bob



# Central Authority Process

---



- **Links information asset sources and sinks**
  - **Can be used to determine transitive information dependencies**
  - **Provides the capability to immediately notify downstream information consumers when an incident occurs**
  - **Consuming organizations periodically download an encrypted message from the central authority**
  - **Possible to calculate an aggregate enterprise-wide valuation for each information asset**
  - **Consuming organizations are now accountable for identifying critical information resources**
-



# Sun Tzu

---



*“The enlightened ruler is heedful, and the good general full of caution.”*

---



# Information Valuation

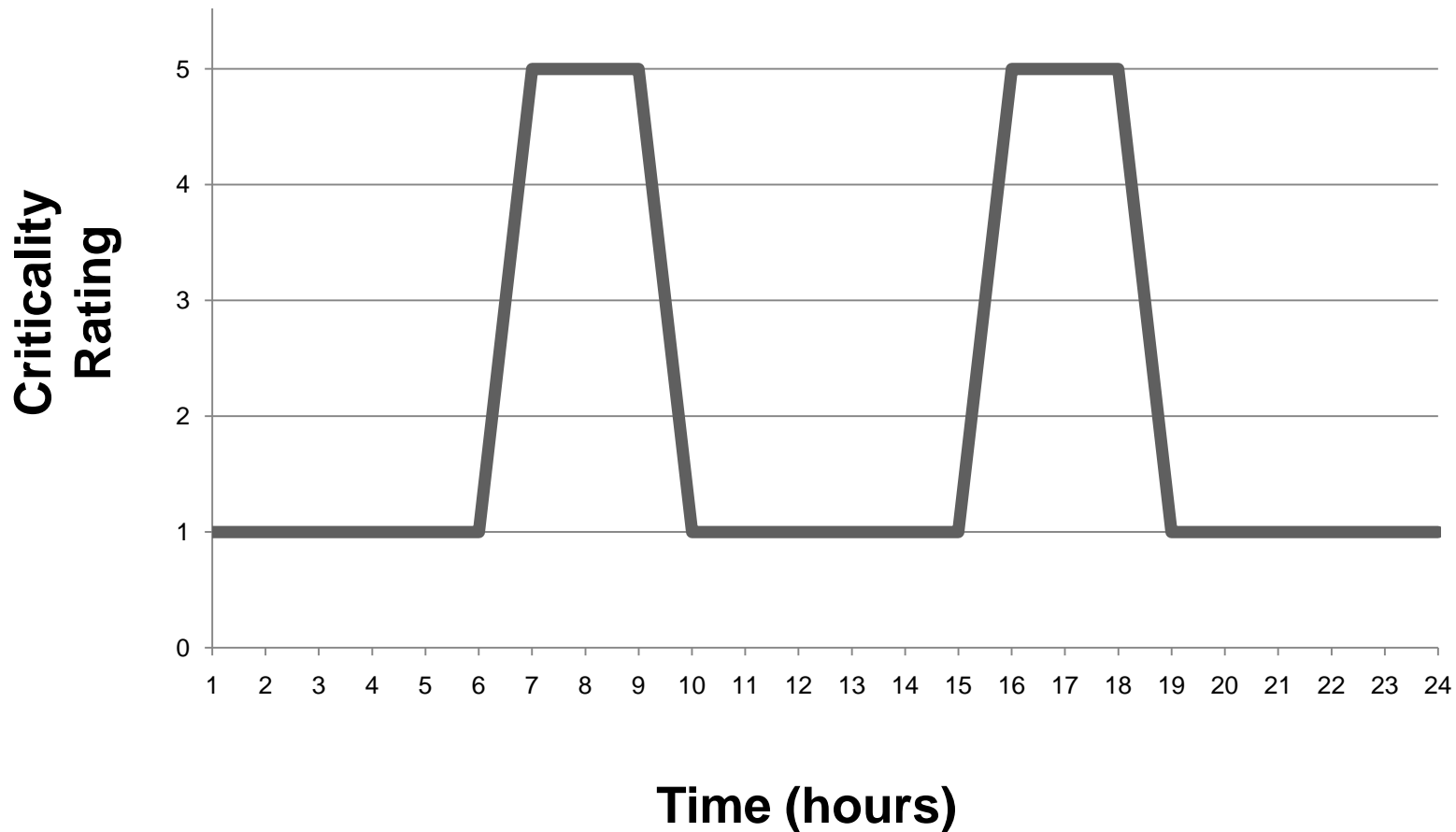
---



- **Information has contextual value**
    - **Frame of reference dependent**
  - **The value of information is relative to the degree in which it supports goal achievement**
    - **Time constraints**
    - **Spatial constraints**
    - **Mission dependent**
  - **No canonical measures of mission achievement**
  - **Decision makers ultimately decide what mission success, degradation, and failure is**
-

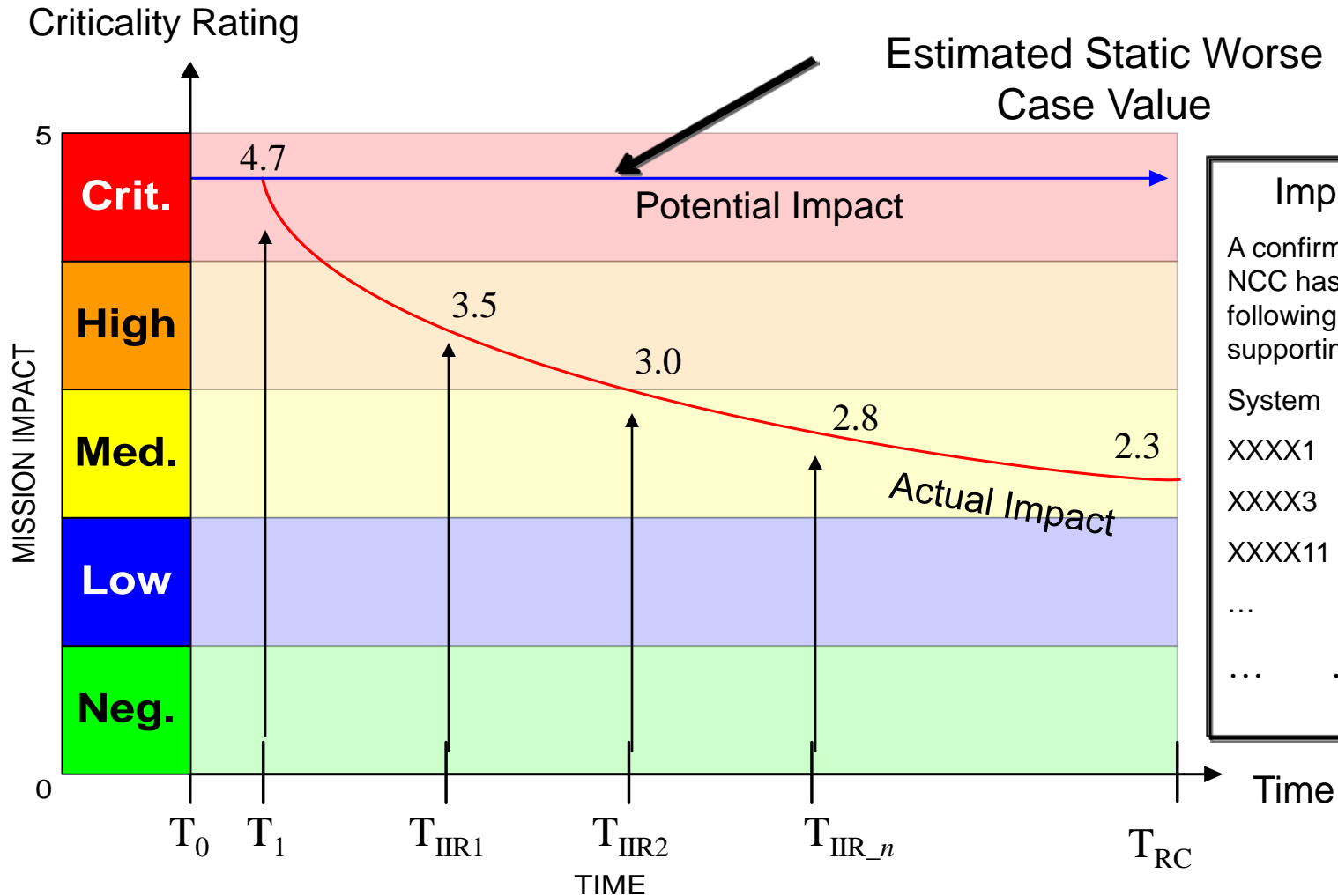


# Temporal Variation of Information Value





# Mission Impact Estimation as a Function of Time (Static)



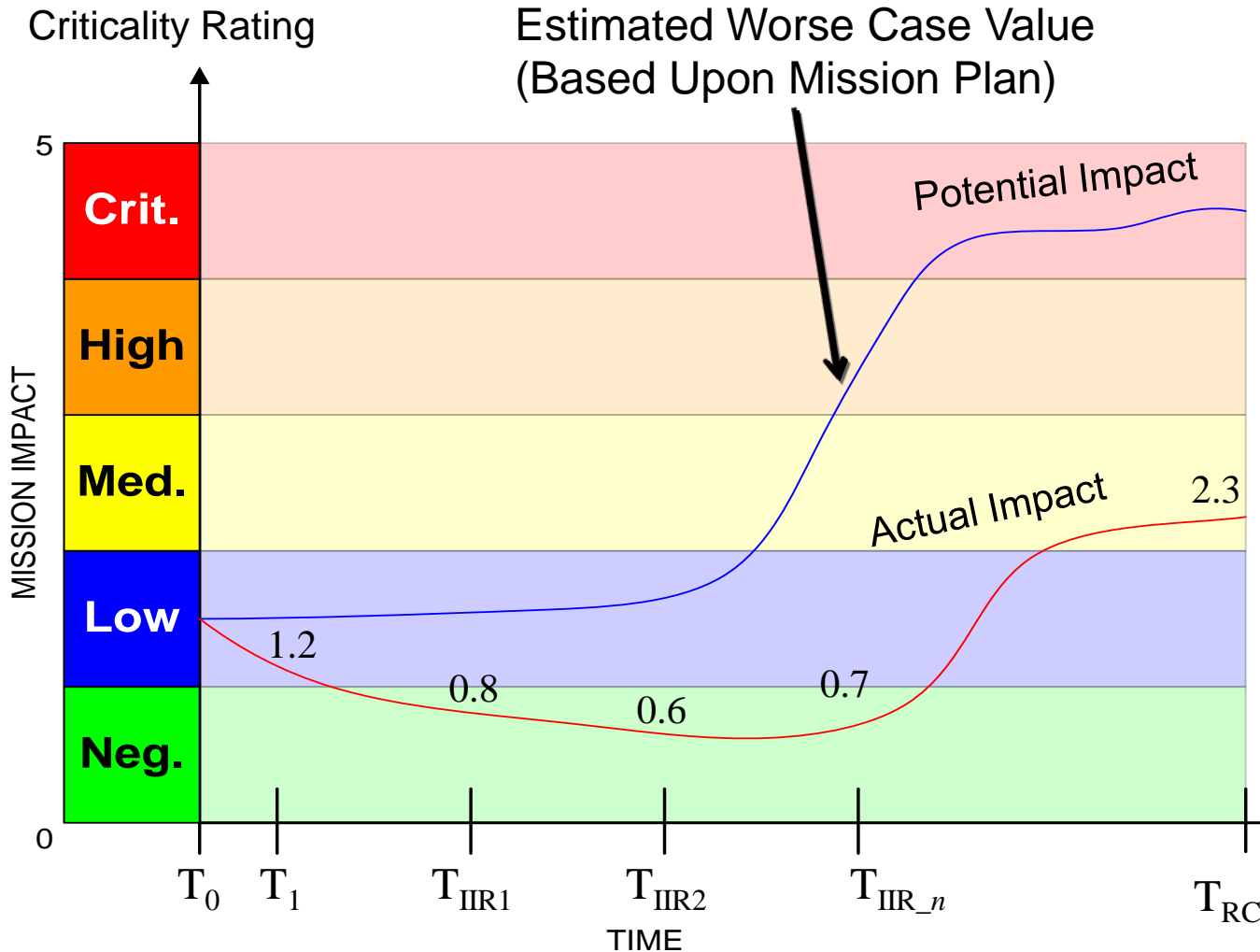
## Impact Summary:

A confirmed data spill at Mosul NCC has resulted in the following compromised mission supporting systems:

System	Est	Mission
XXXX1	4	UAV Feed
XXXX3	4	Convoy Mvmnt
XXXX11	3	Personnel Data
...	...	...
...	...	...



# Mission Impact Estimation as a Function of Time (Dynamic)



## Impact Summary:

A confirmed data spill at Mosul NCC has resulted in the following compromised mission supporting systems:

System	Est	Mission
XXXX1	4	UAV Feed
XXXX3	4	Convoy Mvmnt
XXXX11	3	Personnel Data
...	...	...
...	...	...



# Sun Tzu

---

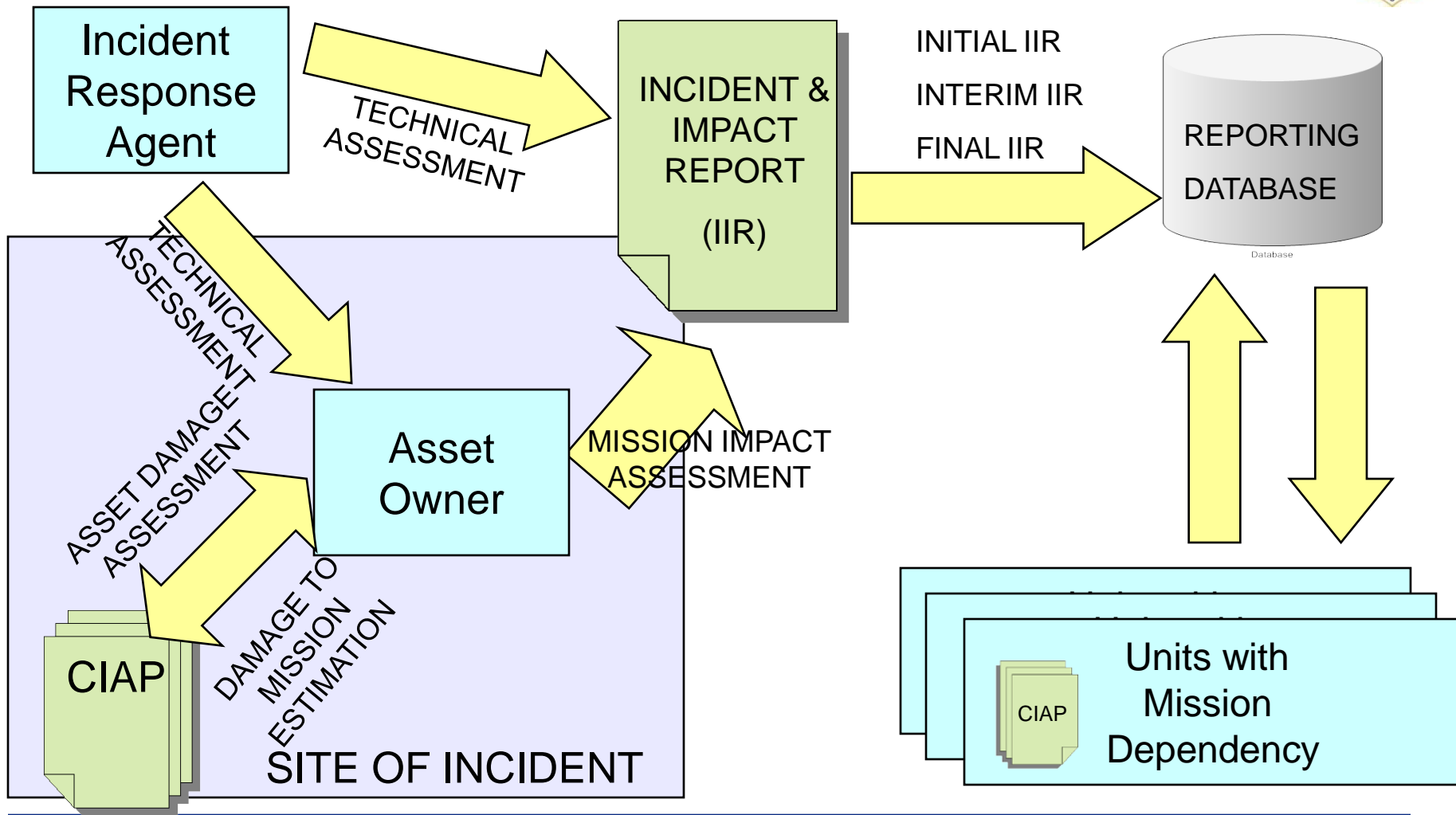


*“The general who wins the battle makes many calculations in his temple before the battle is fought. The general who loses makes but few calculations beforehand.”*

---

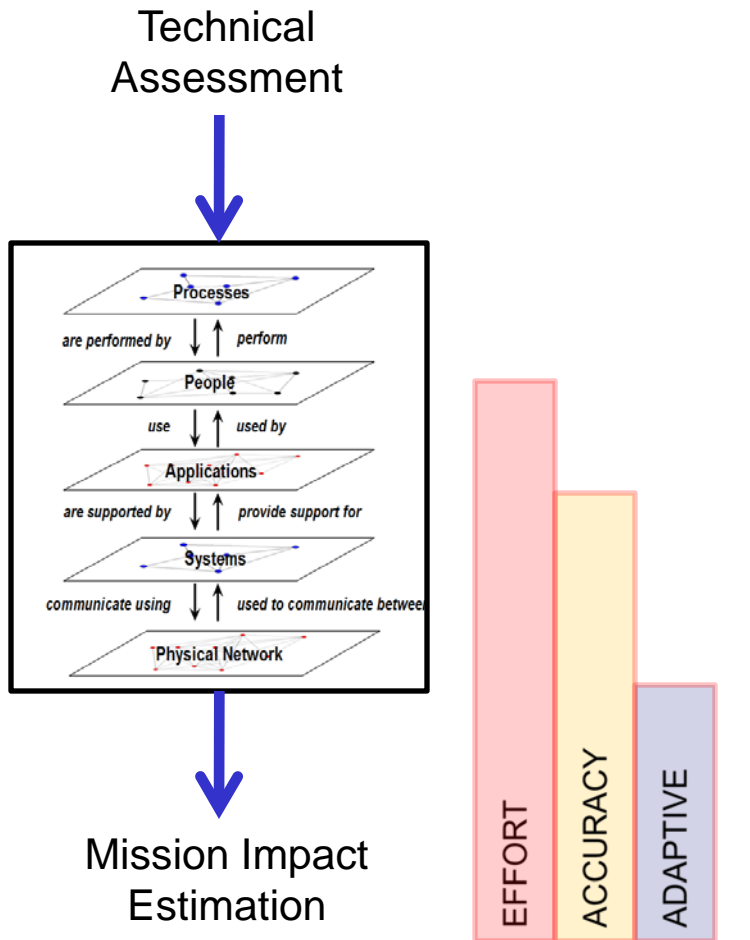


# Conceptual CIMIA Reporting

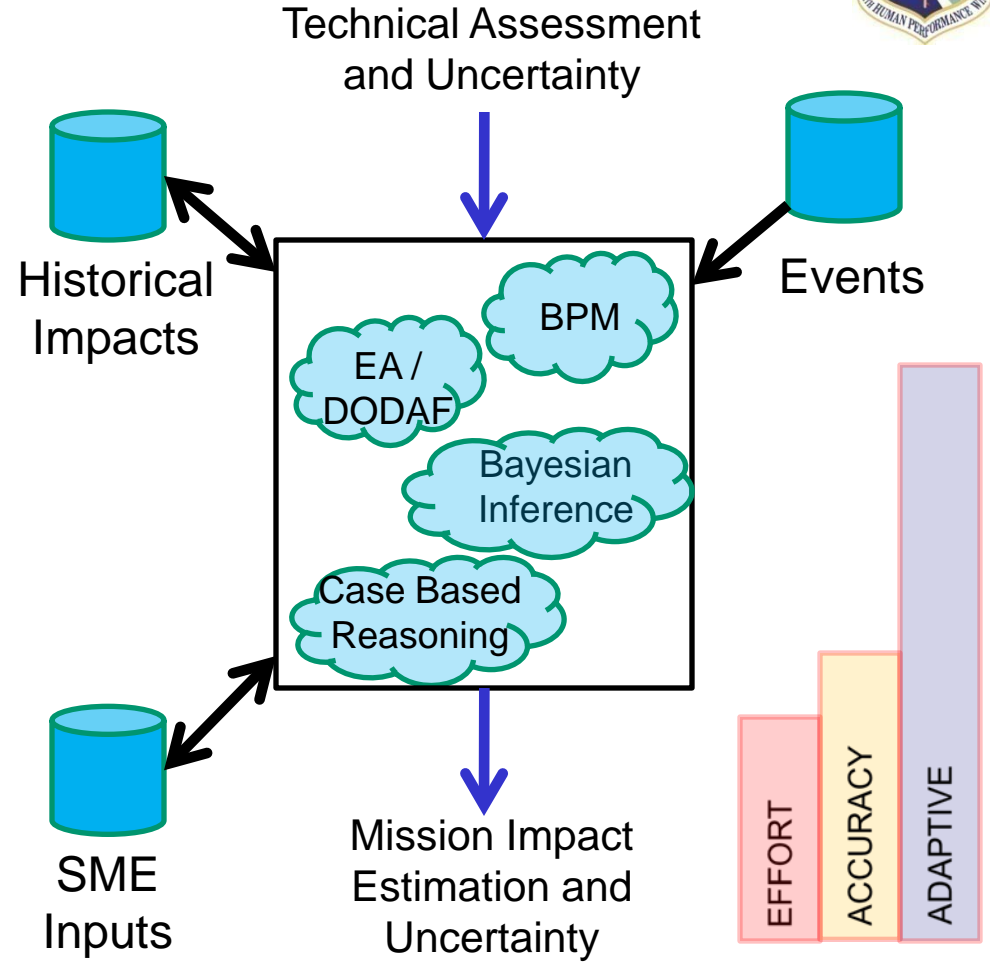




# A Tale of Two Approaches



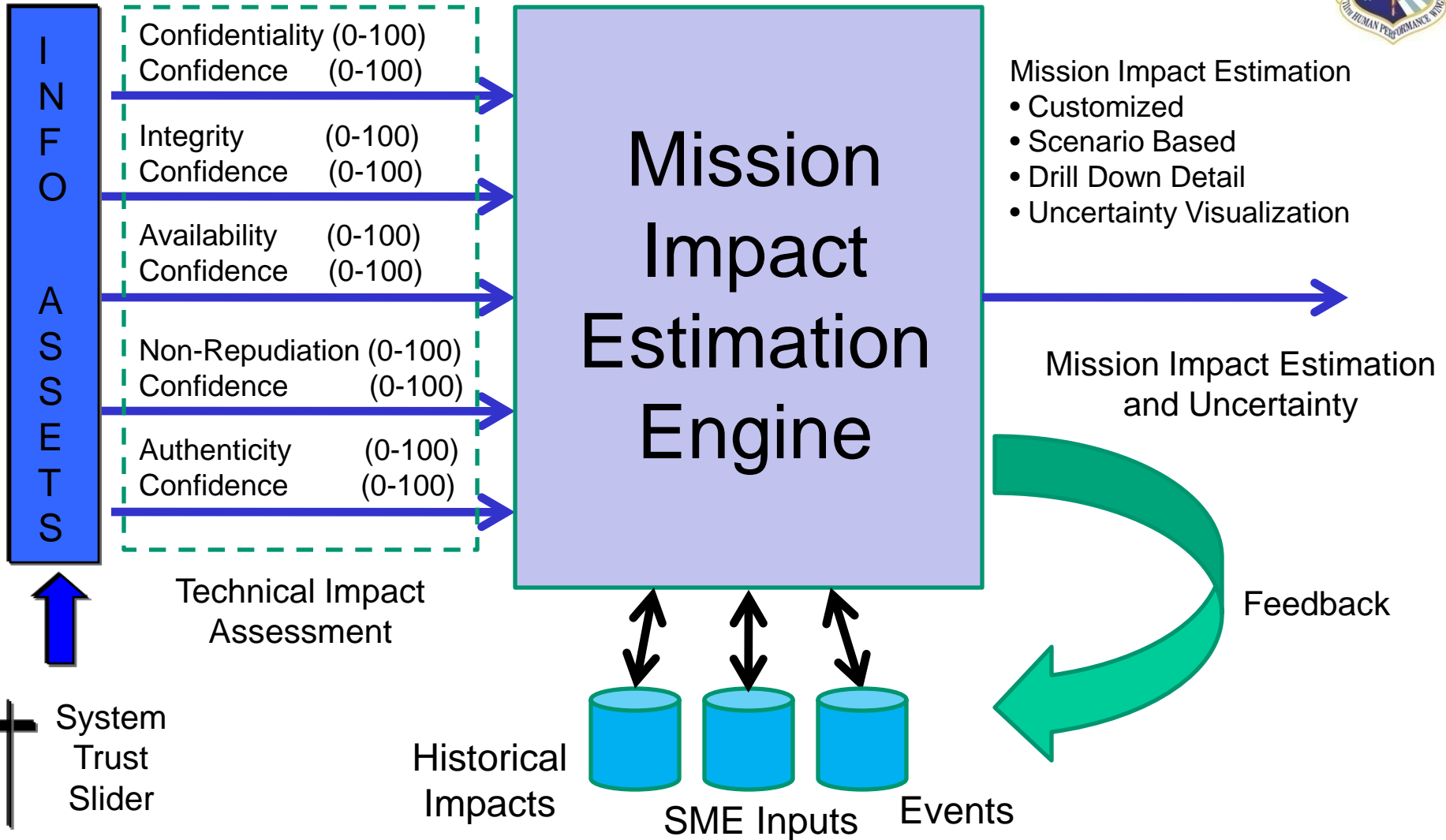
Rigid, Static, Lacks Accounting for Uncertainty



Flexible, Dynamic, Knowledge Retention and Refinement



# Mission Impact Estimation





# CIMIA Research Plan

---



- **Cyber SA evaluation methodology**
  - **Mission representations**
  - **Information asset documentation**
  - **Information valuation**
  - **Knowledge retention and refinement**
  - **Information incident notification process**
  - **Visualization**
  - **Accountability**
  - **Lessons Learned**
  - **All must be realizable, scalable, and secure**
-



# Conclusions



- **CIMIA improves the accuracy, relevance, and timeliness of mission incident impact assessment**
- **We MUST do a better job of accounting for information, its users, and its value**
- **A 50% solution is better than existing methods and provides the basis to improve**
- **Many interdisciplinary issues involved**
- **Helps in understanding adversarial actions**
- **We are currently working on:**
  - **A “proof of concept” experiment**
  - **Mission models (e.g., BPM, workflow models, METLs)**
  - **An evaluation framework to assess any cyber situational awareness solutions**



# Albert Einstein

---



*“We can't solve problems by using the same kind of thinking we used when we created them.”*

---



# Questions

---



**Michael R. Grimaila, PhD, CISM, CISSP, NSA IAM/IEM**  
**Center for Cyberspace Research**  
**Air Force Institute of Technology**  
**Wright-Patterson AFB, OH 45433-7765**  
**Michael.Grimaila@afit.af.mil**

---