# Mission Impact/Threat Assessment for the Cyber Domain

**23 May 2012**


**George Tadda**
**Senior Computer Scientist**
**Air Force Research Laboratory**

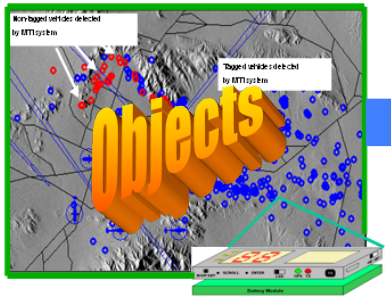
# Overview

- Motivation
- Approach
- Implementation Concepts

# Motivation
## (Reality of Most Environments)

Today WE Have…

Tactical

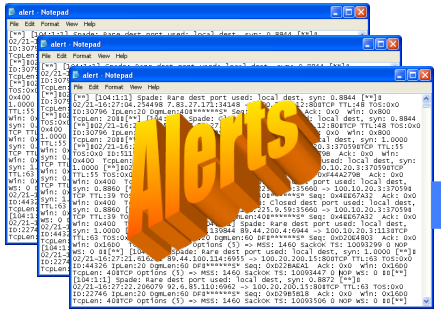



Moving Objects 80/sec
1000's of Objects

Data

The Analyst/Operator


Cyber




Class B Address Space
26,000 Alerts/day

Data

Drowning in data and Inundated with "dots" on map or messages.
INFORMATION STARVED

INCOMPLETE, CONFLICTING DATA

Global


3 – 4 Petabytes/day
(E-mail, Published Pages, etc)

Data

SA is Highly Operator Dependent and 100% Mental Process

- Stress
- Fatigue
- Experience

LIMITED BY INDIVIDUAL'S ABILITIES

…and MORE

# Motivation

## (STEP 1: From Data -> Complex Relations/Situation(s))
## (STEP 2: From Complex Relations/Situation(s) -> Anticipation)

Today WE Have…

Tactical

Cyber

Global

SPATIAL
(Obj Types/No.)

Knowledge Of Units

Data Information

Sensemaking
What is…

Plausible Futures
(Intent, Opportunity, Capability)

Information Assessment

Anticipation
Most Likely/
Most Dangerous eCOA

Weapons Proliferation

TRENDS
(Network, Host)

Knowledge Of Atcks

ALERTS

Data Information

Plausible Futures
(Intent, Opportunity, Capability)

Information Assessment

TRENDS
(Economic, Military)

Knowledge Of Sits

EVENTS

Data Information

Plausible Futures
(Intent, Opportunity, Capability)

Information Assessment

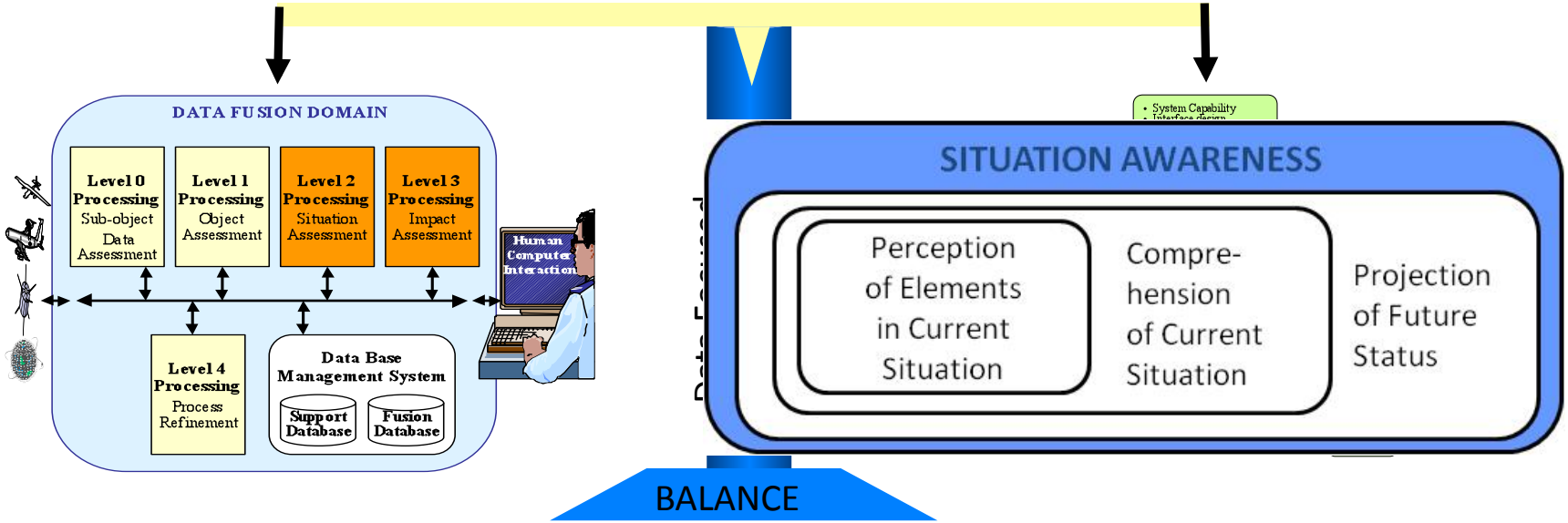
Weapons of Mass Destruction

…and MORE

# Approach
## (Bottom-Up/Top-Down Models)

FUSION

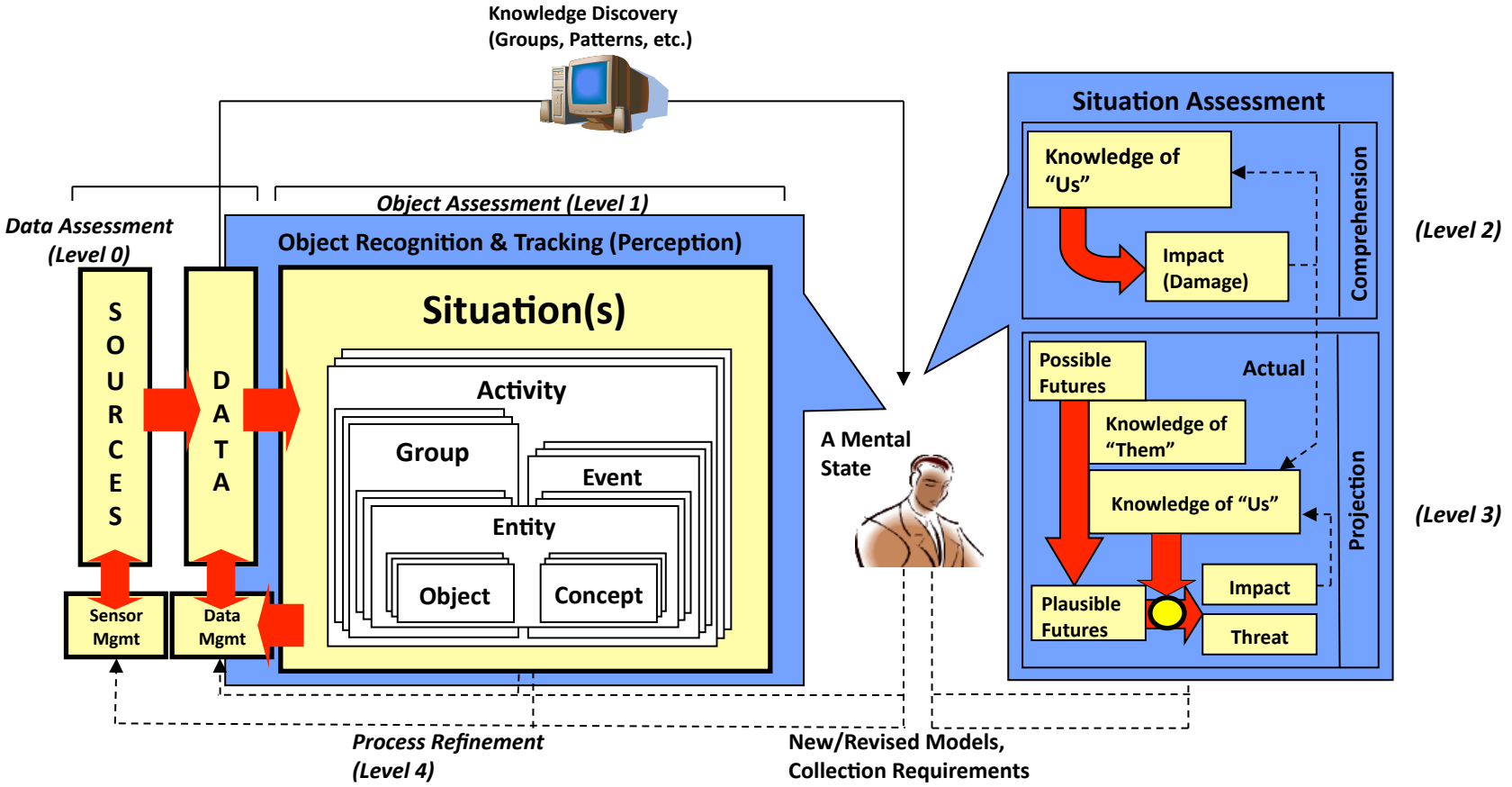
SITUATION AWARENESS




- Most popular is the Joint Director's of Laboratory (JDL) Model (Sensor-based)
- Functional Model
- 5 Levels (Level 0, 1, 2, 3, 4)
- Published By Llinas, Hall, White (1992)
- Most work concentrated on Level 0/1/4 (Dots on Map)
- Little definition of Level 2/3 (What do they mean?)
- Bottom-up, Data Driven

- Receiving Much Attention Today from the Cognitive Community
- Mental Model
- 3 Levels: Perception, Comprehension, Projection
- Developed by: M. Endsley (1995)
- Extended by McGuinness and Foy for Resolution
- Top Down, Goal Driven

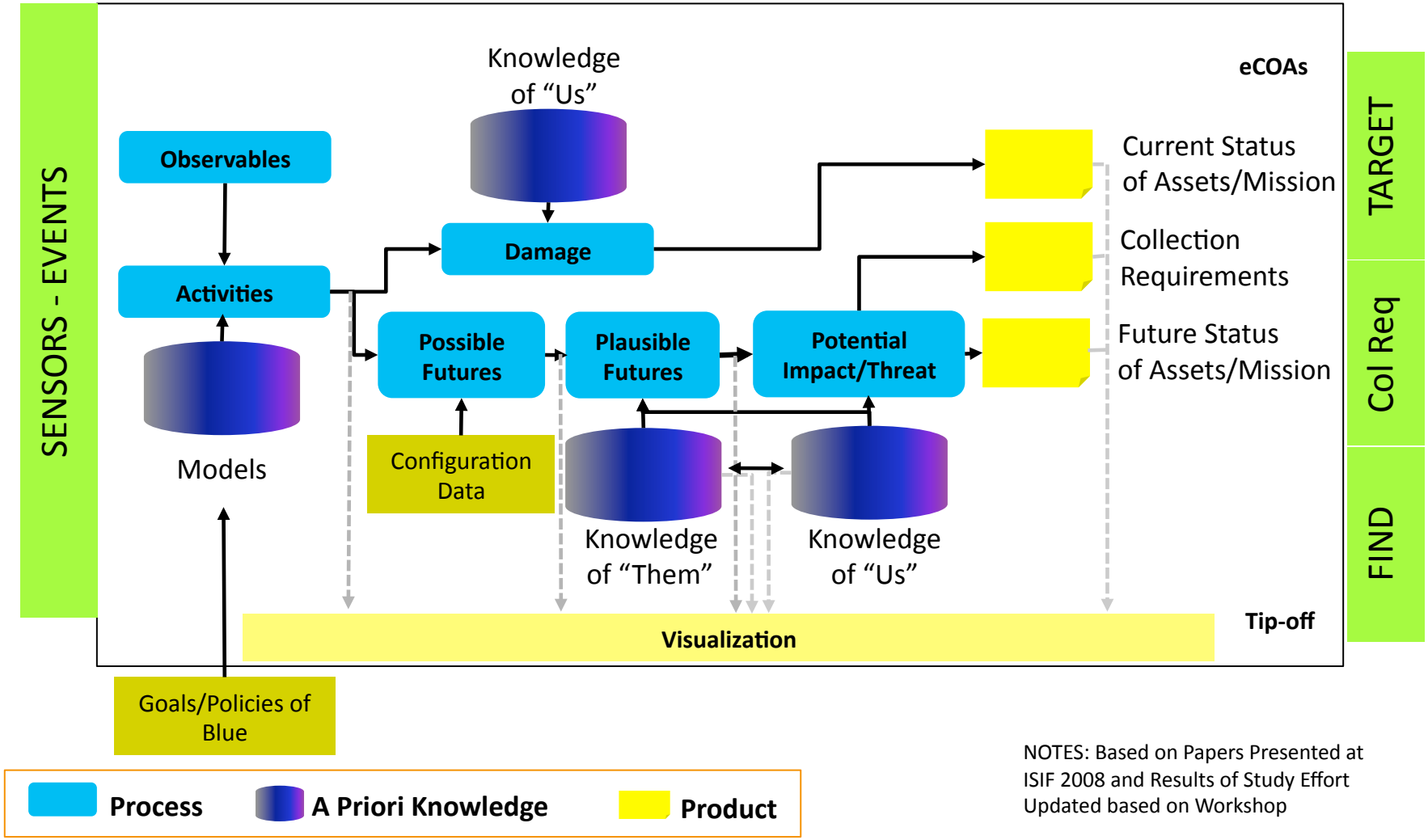
# Approach
## (Situation Awareness Reference Model)



# Situation Awareness Process Model

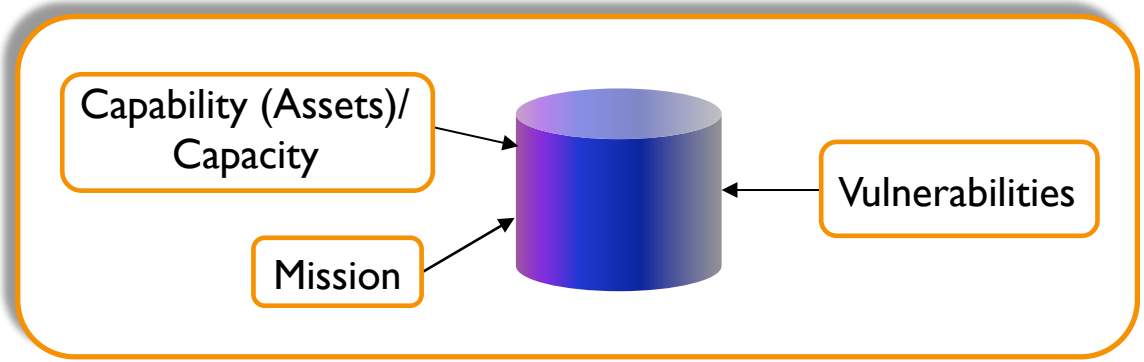
## (Where can automation help?)

From Observables to Threats (At Time, t)




NOTES: Based on Papers Presented at ISIF 2008 and Results of Study Effort Updated based on Workshop

# Knowledge of "Us"




- **Each mission, each asset, and each vulnerability has a state variable representing its operational status at a given time**
- **The knowledge of us also involves relationships between the entities, including:**
  - **Each asset can be associated with one or more missions**
  - **The accessibility or dependency between the assets**
  - **An asset can have multiple vulnerabilities, each has different effect to the asset's operational capability**
  - **Each asset may have multiple state variables (e.g., a server can be discovered and still be operational)**
- **The vulnerabilities shall be associated with potential observables to be deduced from adversary (or blue's, or incidental) activities**

# Current Impact Assessment

- Current Impact Assessment (the upper thread – comprehension or JDL Level 2) is effectively a damage assessment of what is occurring or just recently occurred
- What information is needed to accomplish this assessment?
  - Effected aspect(s) of the ‘asset’
  - Use of the ‘asset’ (or aspect) towards fulfilling the ‘mission’ or task
  - Roll up of the ‘effect’

# Plausible Future Impact/Threat Assessment

**Two information needs for the 'lower thread' – projection or JDL Level 3:**

- **Information to perform impact assessment on projected future activity (this information is essentially identical to that needed for current impact assessment)**
- **Information to analyze and constrain possible futures to plausible futures; what is the information need?**
  - **Knowledge of 'Us'**
    - Vulnerabilities
    - 'Terrain'
    - Configuration
    - Mission Map
  - **Knowledge of 'Them'**
    - Capability
    - Capacity
    - Opportunity
    - Intent

# Technical Challenges

- **Knowledge of Us is essentially an information store and most of the information exists**
- **Greatest technical challenge for Knowledge of Us is information relevancy**
  - **Must be current, accurate, easy to acquire/update**
  - **Automated as much as possible**
  - **Dynamic**
- **Challenges for Knowledge of Them are similar but are further complicated by the information being sparse and difficult to obtain**

# Mission Mapping Abstractions

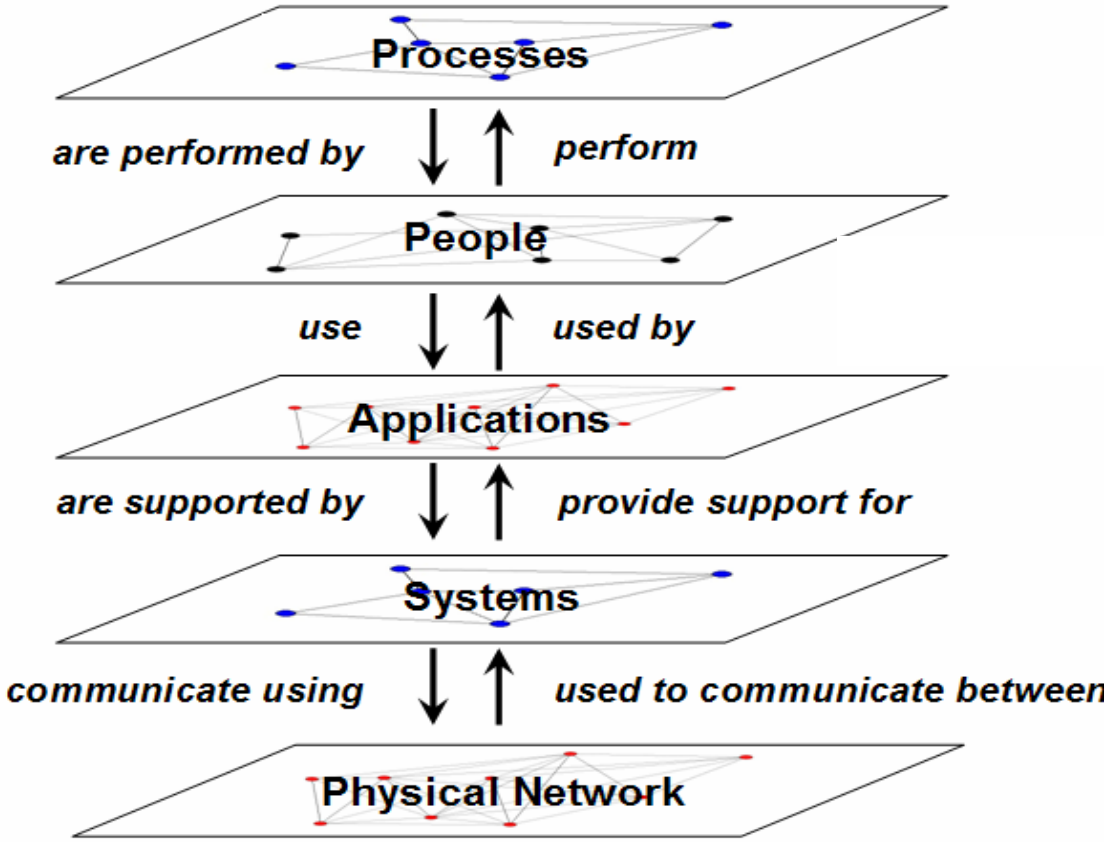
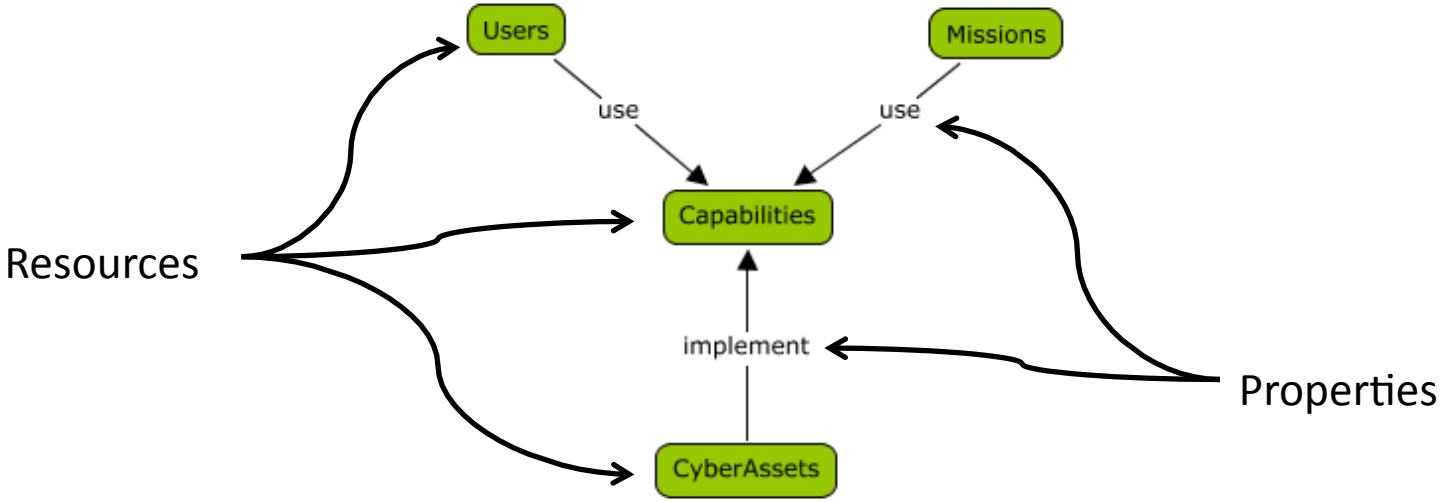


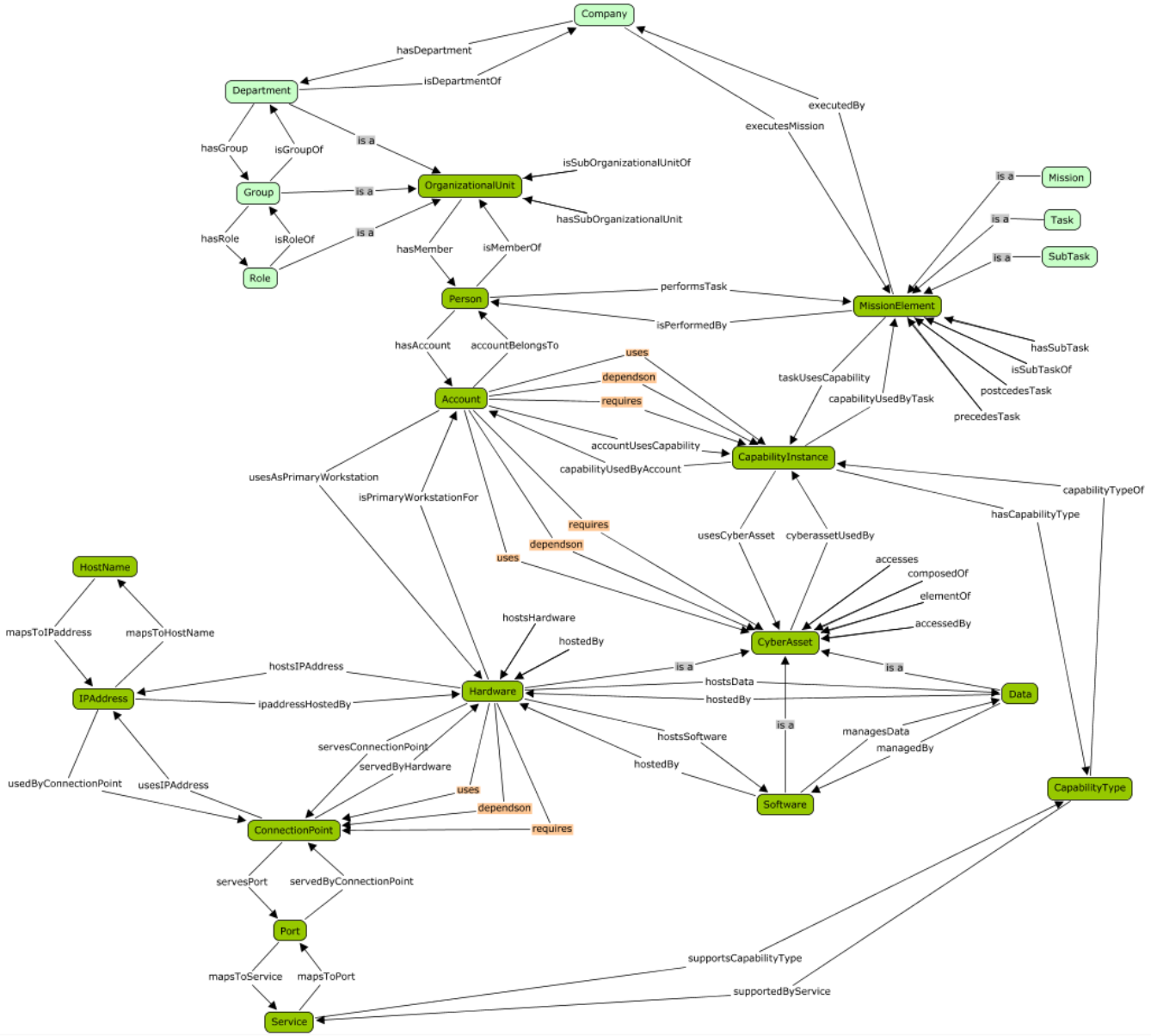

Figure reference; M. R. Grimaila, R. F. Mills, and L. W. Fortson, *An Automated Information Asset Tracking Methodology to Enable Timely Cyber Incident Mission Impact Assessment*, 13th International Command and Control Research and Technology Symposia (ICCRTS 2008), 17-19 Jun 2008, Seattle, WA.

# Ontology

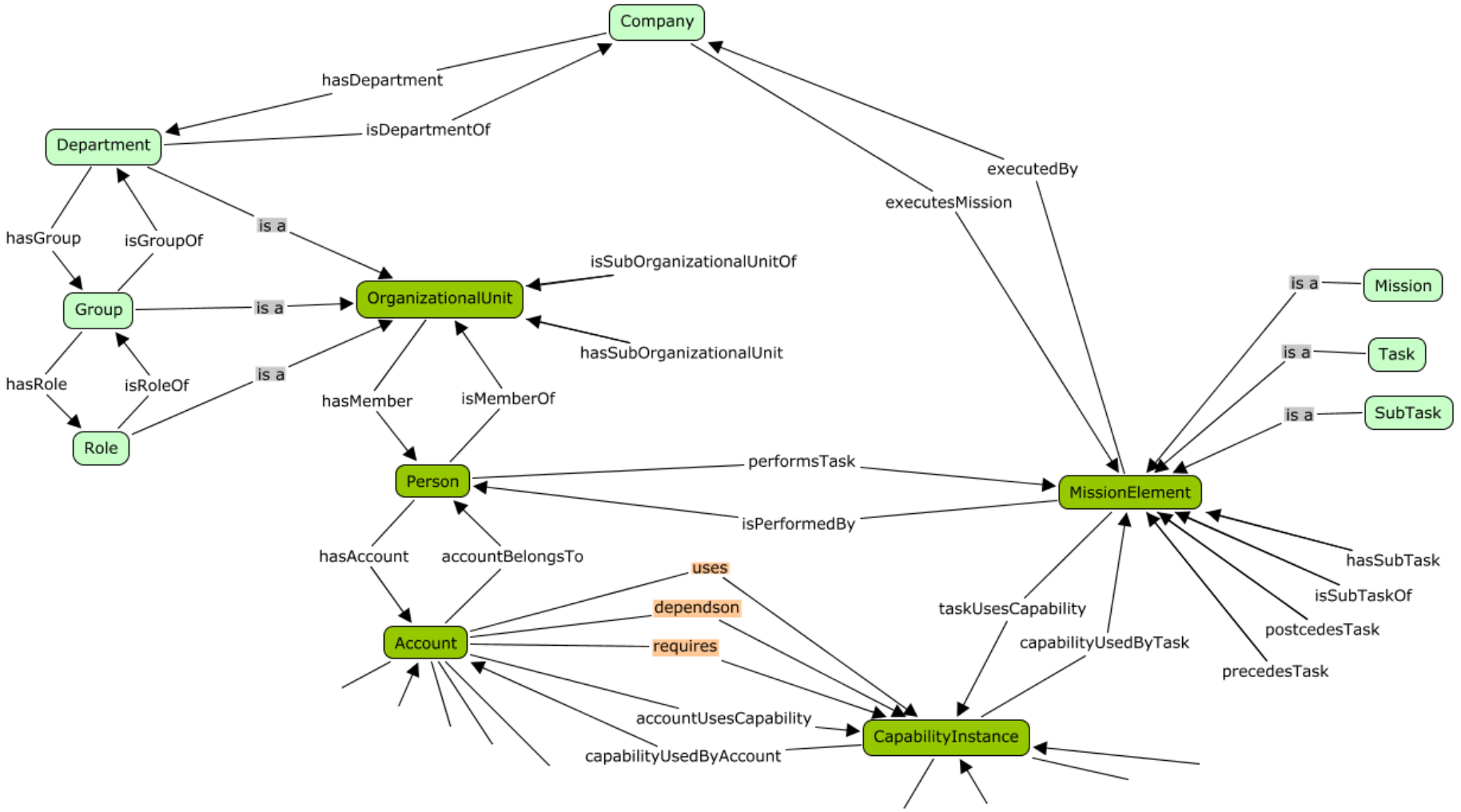



Ontology reference: A. D'Amico, L. Buchanan, J. Goodall, P. Walczak, *Mission Impact of Cyber Events: Scenarios and Ontology to Express the Relationships between Cyber Assets, Missions and Users*, 5th International Conference on Information Warfare and Security, 8-9 Apr 2010, Dayton OH.

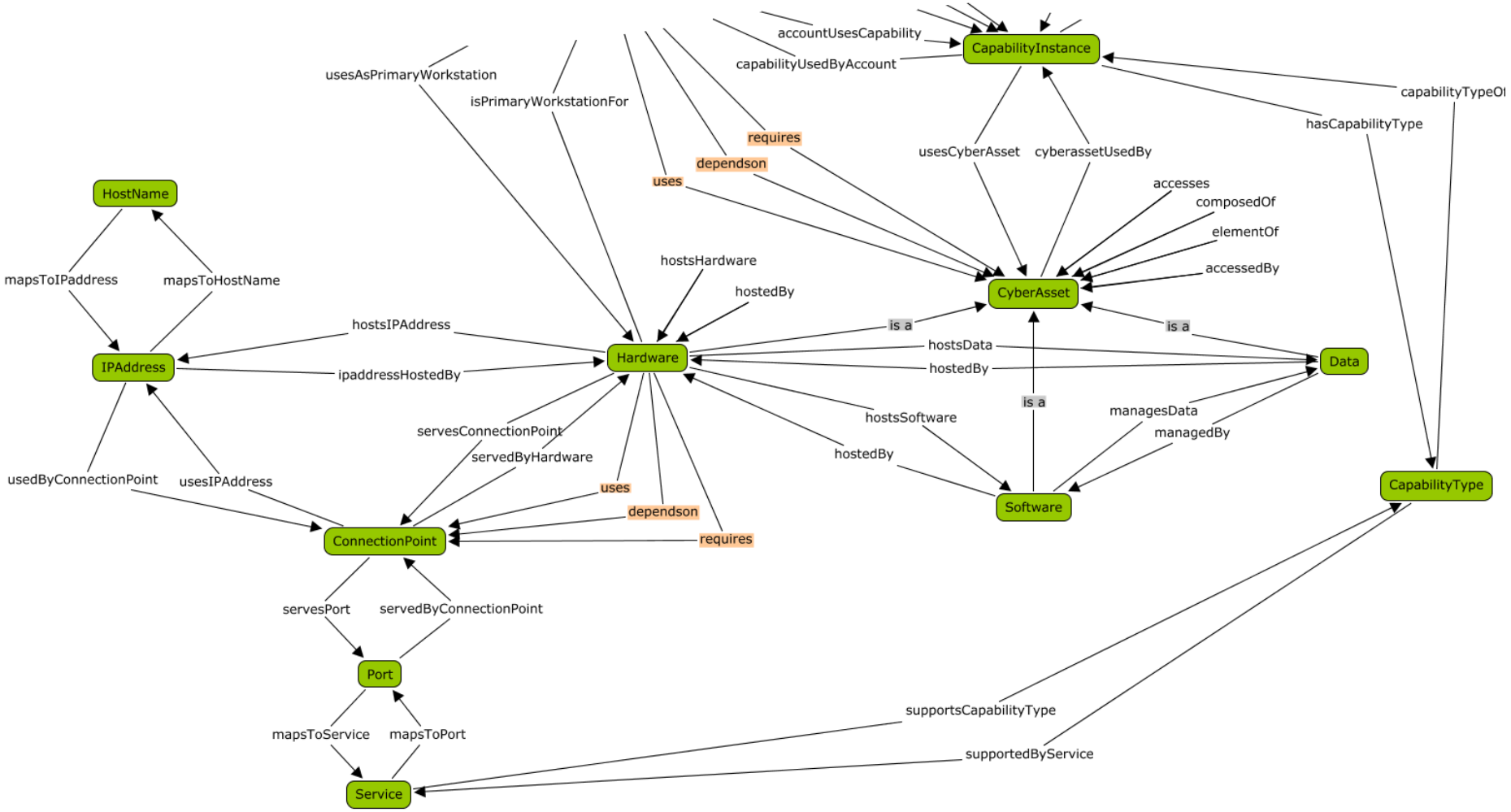
# Ontology (2)



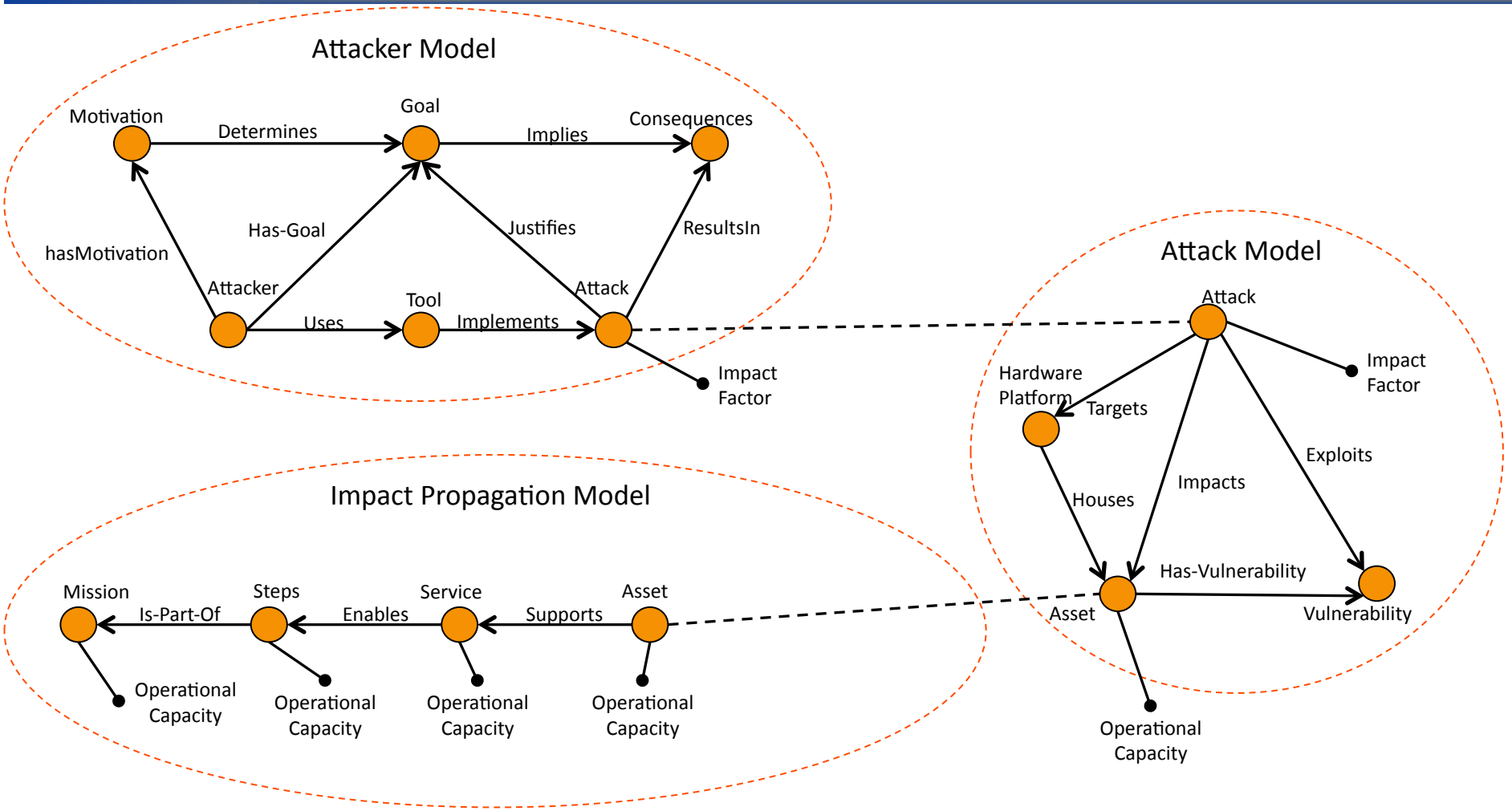
# Ontology (3)



# Ontology (4)

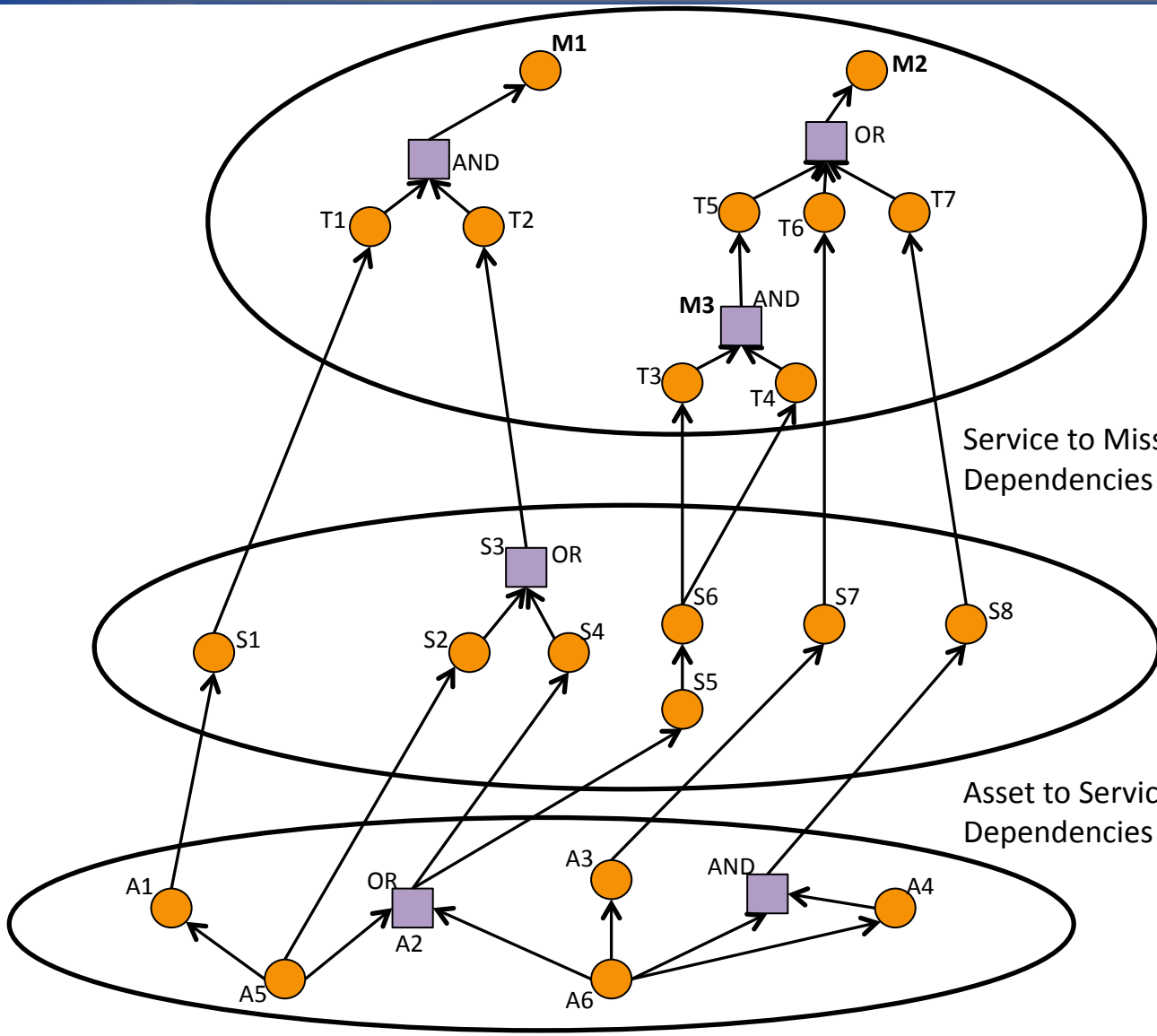


# Cyber Security Incident Model




Reference: G. Jakobson, *Extending Situation Modeling with Inference of Plausible Future Cyber* Situations, 2011 IEEE First International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support, 22 – 24 Feb 2011, Miami Beach FL.

# Impact Dependency Graph




Intra-Mission Dependencies

Service to Mission Dependencies

Intra-Service Dependencies

Asset to Service Dependencies

Intra-Asset Dependencies

# Effect/Impact Propagation

- **Impact Factor (IF) is a measure from the interval [0, 1] which indicates the how much an attack is capable of compromising an asset where 0 is no impact and 1 means there is no operational capacity**
- **Operational Capacity (OC) is a measure from the interval [0, 1] which indicates the level of compromise with 0 meaning totally compromised and 1 meaning fully operational**

Then to calculate the operational capacity for an asset **a**, which is under direct attack **x**:

$OC_a(t') := \text{Max}\ [OC_a(t) - IF_x(t'), 0]$

Or, if an asset **a** is effected by attack **x** but not under direct attack

$OC_a(t') = \text{Min}\ [OC_a(t), OC_b(t)]$

Considering the Impact Dependency Graph, can propagate effects using the following formulas for OC:

$OC_{OR}(t) = \text{AVE}(OC_1(t), OC_2(t), \ldots, OC_n(t))$

$OC_{AND}(t) = \text{MIN}(OC_1(t), OC_2(t), \ldots, OC_n(t))$

# Summary

- Motivation
- Approach
- Implementation Concepts