Computational Theory and Cognitive Assistant for Intelligence Analysis

Gheorghe Tecuci, David Schum, Mihai Boicu, Dorin Marcu, Katherine Russell

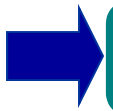
Learning Agents Center, George Mason University

http://lac.gmu.edu

The Sixth International Conference on Semantic Technologies for Intelligence, Defense, and Security – STIDS

Fairfax, VA, 17 November 2011

Overview



- Computational Theory of Intelligence Analysis
- Hypotheses Analysis with TIACRITIS
- Cyber Insider Threat Discovery and Analysis
- Future Research and Development
- Discussion

Computational Theory of Intelligence Analysis


Aristotle


Galileo


Newton


Locke


Whewell


Peirce


Wigmore

Hypothesis

Likelihood of Hypothesis

Evidence marshaling

What hypothesis would explain these observations?

(Abduction: O → possibly H)

Hypothesis-driven collection

What evidence is entailed by this hypothesis?

(Deduction: H → necessarily E)

Multi-INT fusion

What is the likelihood of the hypothesis?

(Induction: E → probably H)

Observations

New Evidence

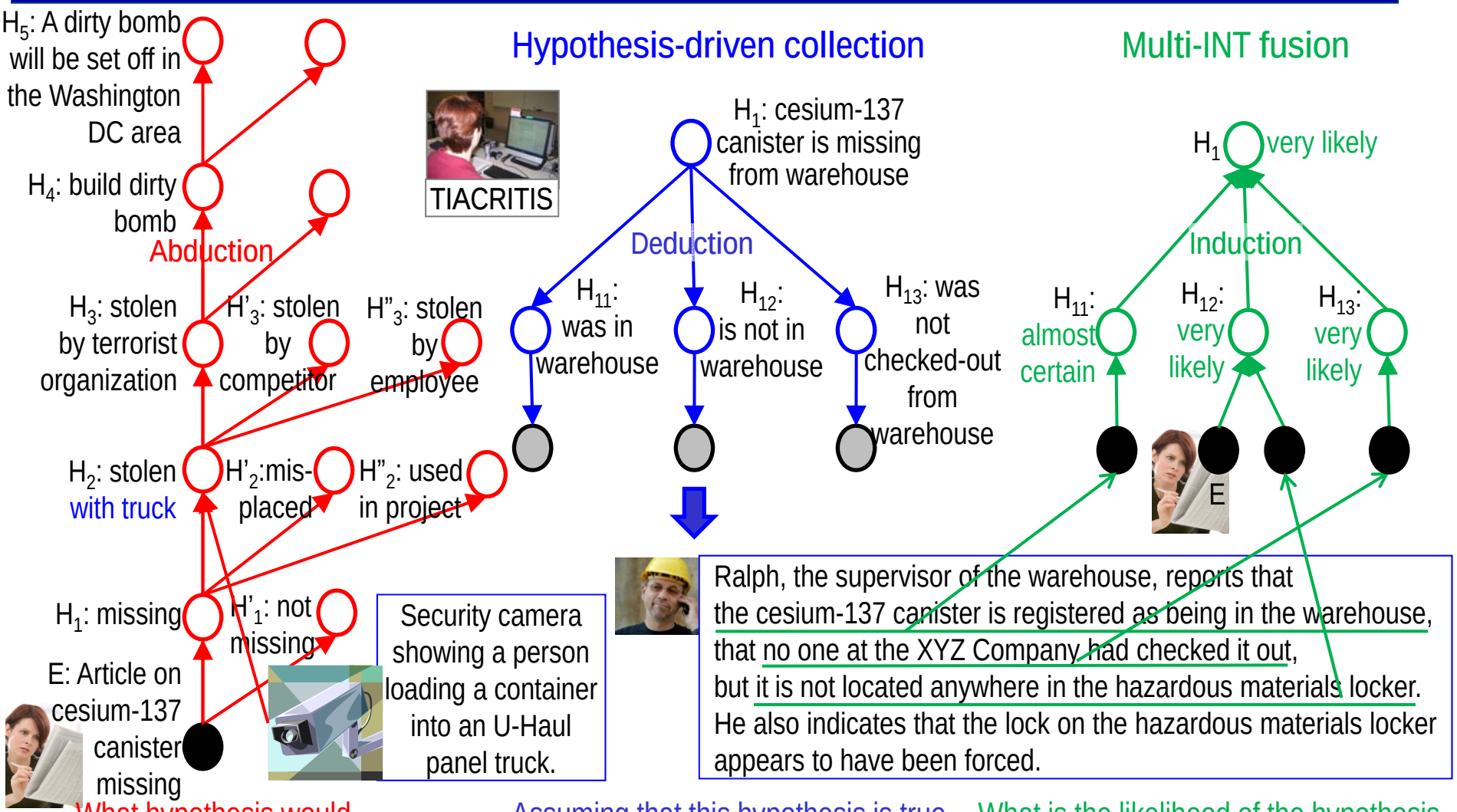
Evidence in search of hypotheses

Hypotheses in search of evidence

Evidentiary tests of hypotheses

Implemented in TIACRITIS, a Disciple and web-based cognitive assistant that supports analysts in coping with the astonishing complexity of intelligence analysis.

Discovery of Evidence, Hypotheses, and Arguments



Hybrid spiral reasoning

Learning analytic expertise

H_5: A dirty bomb will be set off in the Washington DC area

H_4: build dirty bomb

H_3: stolen by terrorist organization

H_2: stolen with truck very likely

H_1: missing very likely

E: Article on cesium-137 canister missing

H'_2:mis-placed

H''_2: used in project

H'_3: stolen by competitor

H''_3: stolen by employee

H_2: cesium-137 canister stolen with truck — very likely

Hypothesis-driven collection

H_{21}: cesium-137 canister missing from warehouse — very likely

H_{22}: missing canister stolen with truck — very likely

Heuristic power of evidence-suggested scenarios

Scenario: Truck entered company, canister stolen from locker, canister loaded into truck, truck left with canister.

Truck entered company — almost certain

Cesium-137 canister stolen from locker — almost certain

Cesium-137 canister loaded in truck — very likely

Truck left with canister — very likely

The record, made by Sam, security guard at the XYZ Company, that a panel truck bearing Maryland license plate number MDC-578 was in the XYZ parking area on the day before the discovery of the missing cesium-137 canister.

The lock appears to have been forced.

Locksmith Clyde's reports that the lock was forced.

Multi-INT fusion

Security camera showing a person loading a container into an U-Haul panel truck.

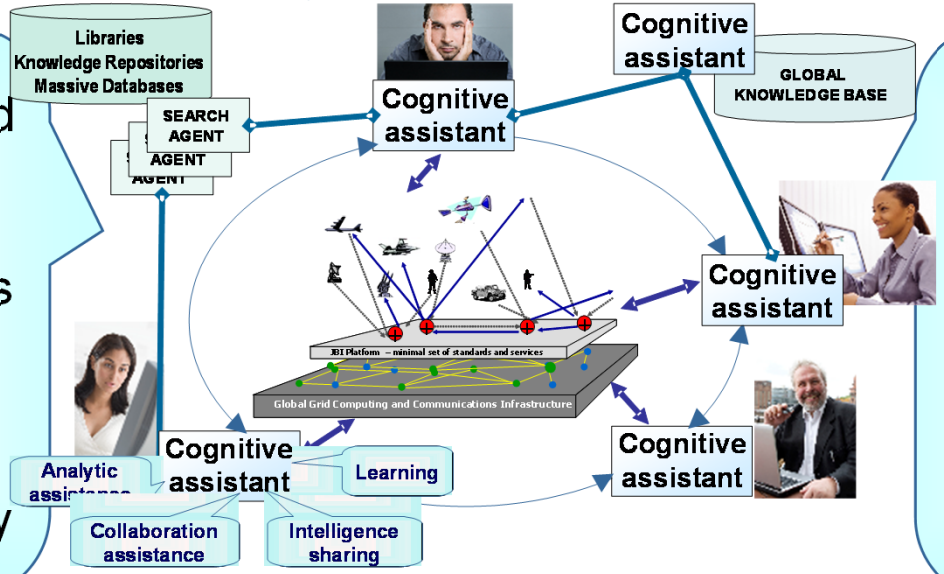
Analyst's Cognitive Assistant: Disciple/TIACRITIS

Analytic Assistance

Supports intelligence analysts with evidence marshaling and hypotheses generation, hypothesis-driven evidence collection, multi-INT hypotheses testing, collaboration with other analysts and experts, and intelligence sharing.

Learning

Rapidly acquires and maintains analytic expertise which currently takes years to establish, is lost when experts separate from service, and is costly to replace.



Tutoring

Helps new student analysts learn the critical thinking skills for evidence-based hypotheses generation and analysis, through a hands-on approach

Science of Evidence, Artificial Intelligence Logic, Probability

Textbooks, Courses, Case Studies

Introduction to Intelligence Analysis: A Hands-on Approach	A Practicum in Evidence Marshaling and Argument Construction	Modeling the Behavior of Violent Extremists
13 case studies 4 course versions	In preparation complex case studies	24 case studies 5 course versions

Overview

Computational Theory of Intelligence Analysis

Hypotheses Analysis with TIACRITIS

Cyber Insider Threat Discovery and Analysis

Future Research and Development

Discussion

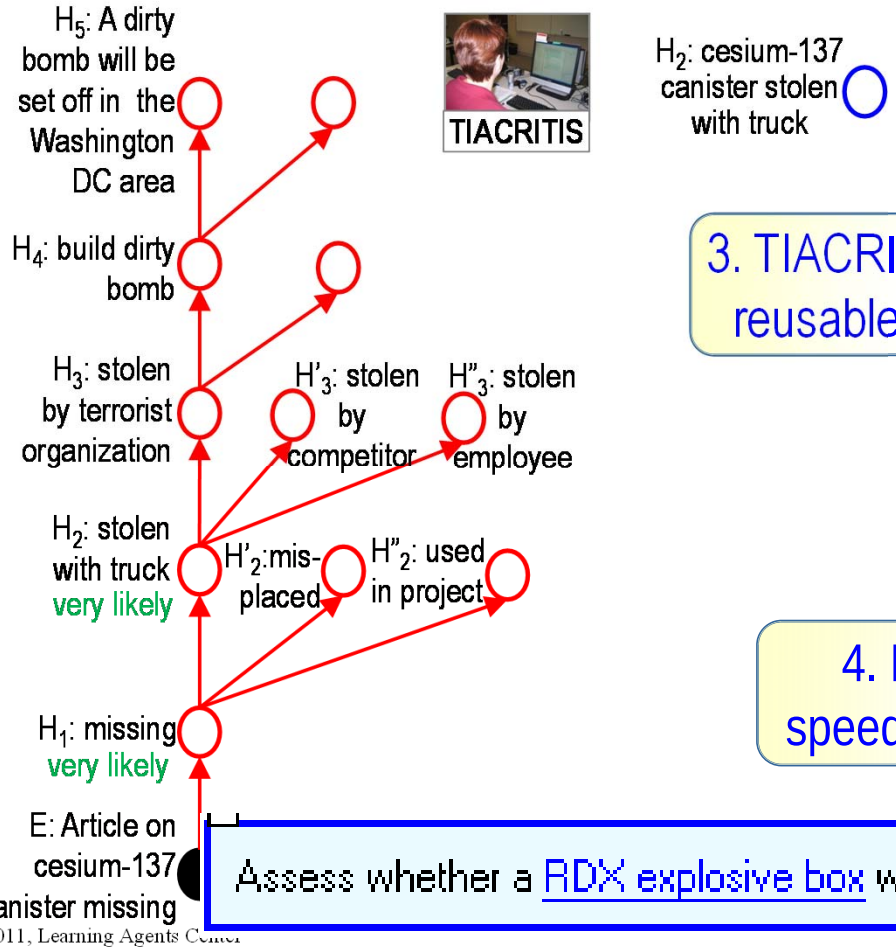
Illustration of the Use of TIACRITIS

Hypothesis Formulation

1. Analyst formulates the hypothesis analysis problem in English

2. Analyst the selects objects and actors

Assess whether a cesium-137 canister was stolen from the XYZ warehouse with the MCD-578 truck.



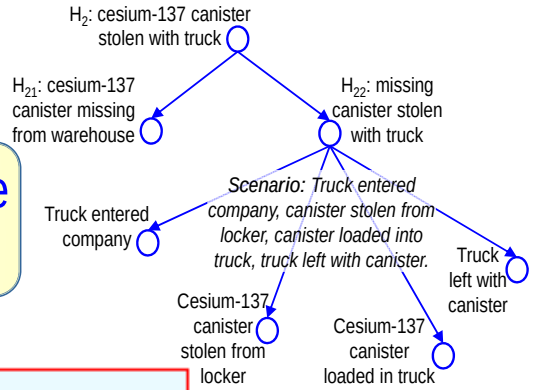
3. TIACRITIS learns reusable patterns

Assess whether a ?O1 was stolen from the ?O2 with the ?O3.

4. Learned patterns speed-up future analyses

Assess whether a RDX explosive box was stolen from the Allied Import with the VA-9867 car.

Hypothesis Decomposition



1. Analyst and TIACRITIS decompose the initial problem down to the level of elementary hypotheses to be evaluated based on evidence

Assess whether a cesium-137 canister was stolen from the XYZ warehouse with the MCD-578 truck.

Q:Which is an assessment strategy?
A:Determine that a cesium-137 canister is missing and that it was stolen with the MCD-578 truck.

2. TIACRITIS learns reasoning patterns from decompositions defined by analyst

Assess whether a cesium-137 canister is missing from the XYZ warehouse.

Assess whether the missing cesium-137 canister was stolen with the MCD-578 truck.

3. TIACRITIS may suggest reformulations to reuse reasoning patterns

4. TIACRITIS may suggest decompositions

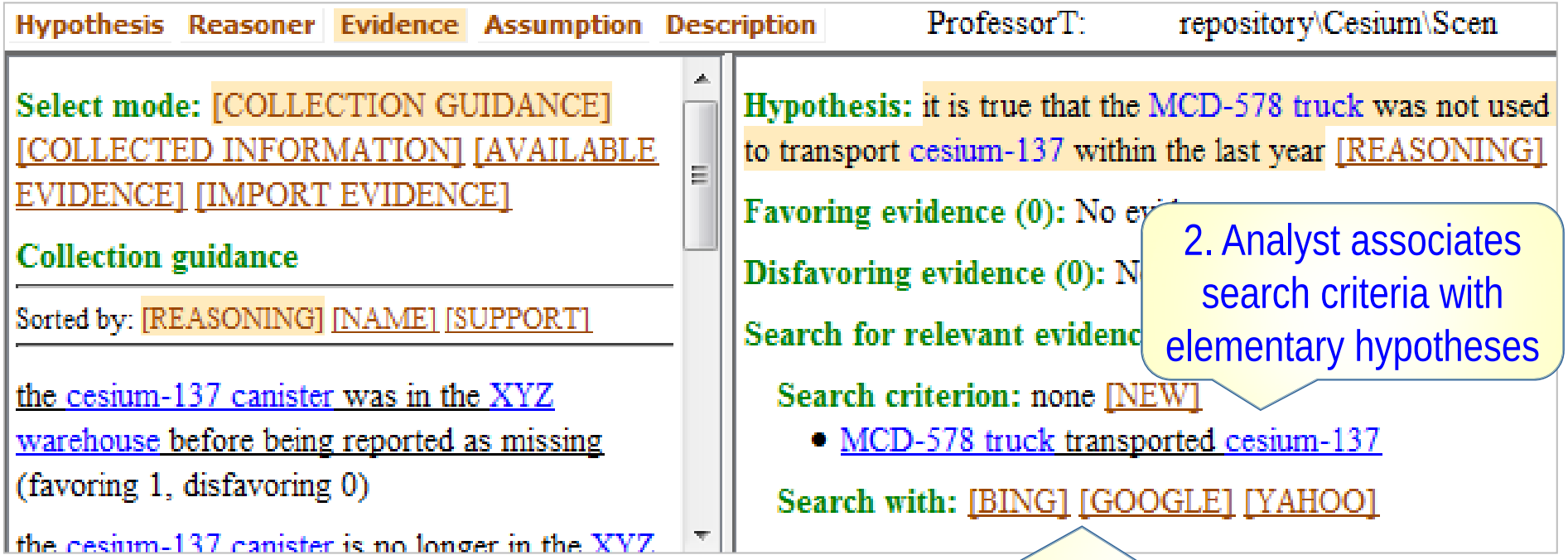
Q:Which is a possible scenario?
A:The MCD-578 truck entered the XYZ warehouse, the cesium-137 canister was stolen from the hazardous mat
loaded into the truck which left with it.

Assess whether the MCD-578 truck entered the XYZ warehouse.

Assess whether the cesium-137 canister was stolen from the hazardous material locker.

Assess whether the cesium-137 canister was loaded into MCD-578 truck.

Evidence Collection

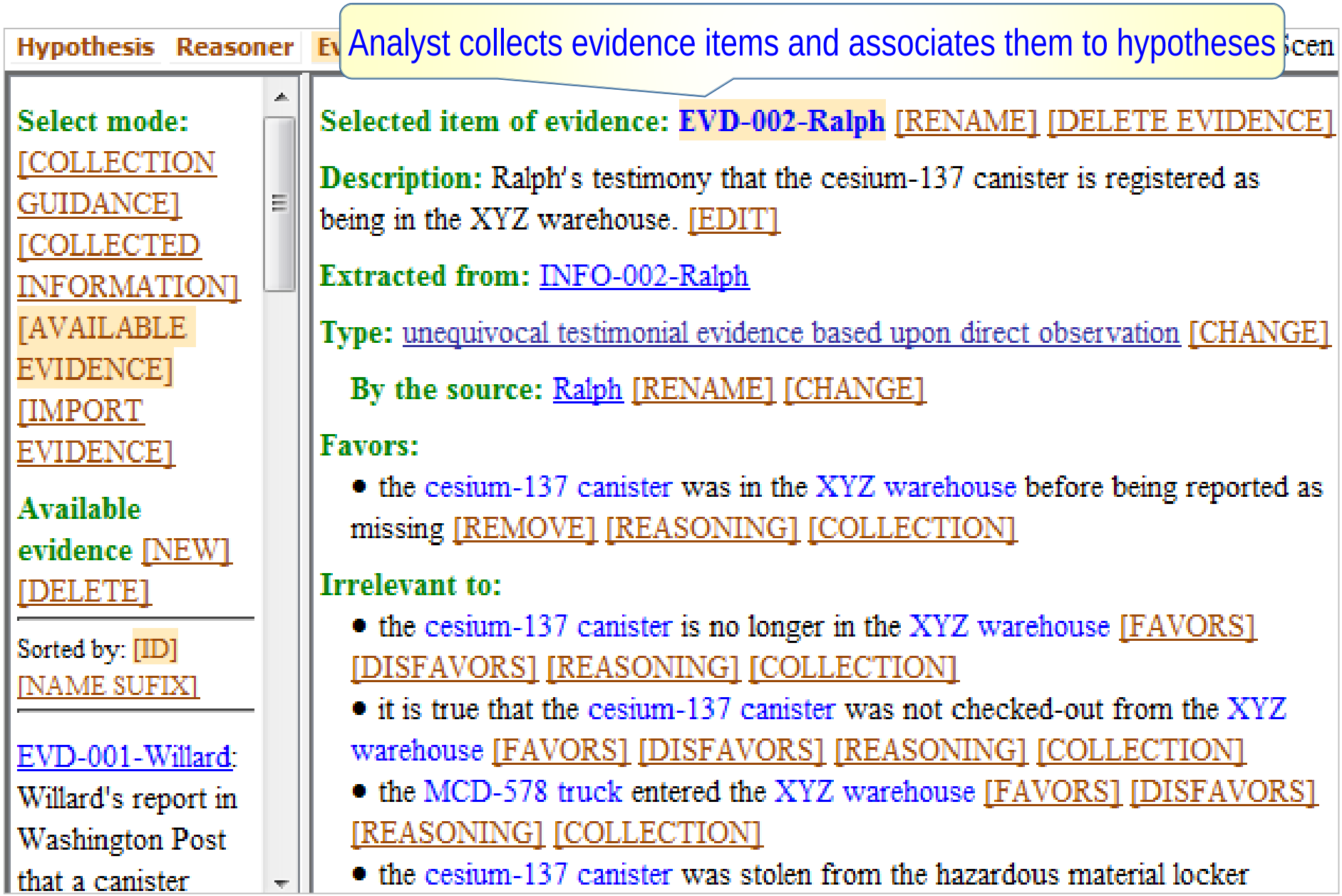


2. Analyst associates search criteria with elementary hypotheses

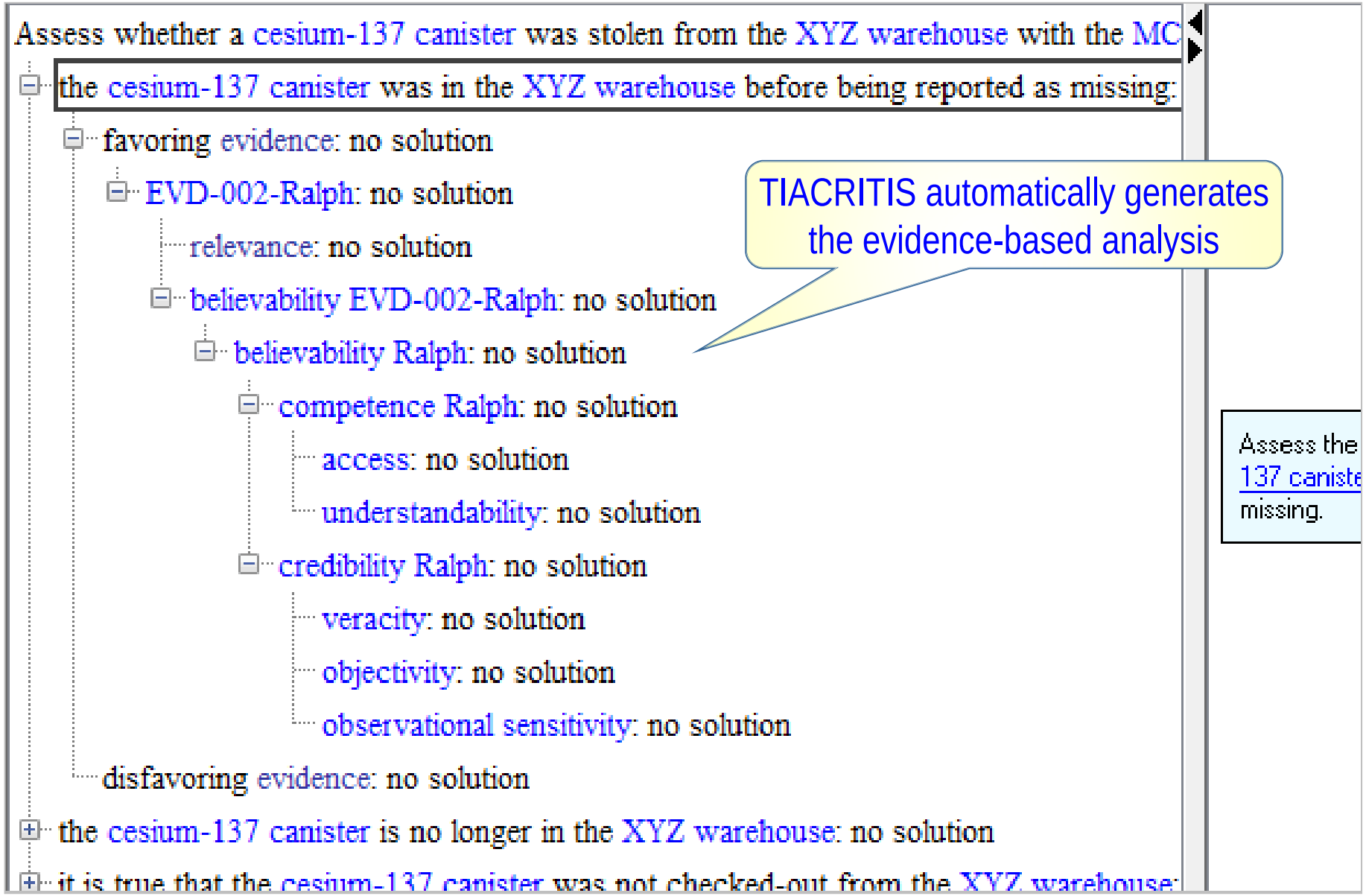
1. Elementary hypotheses to be evaluated based on evidence

3. Search engines are invoked to identify relevant evidence

Evidence Representation and Use



Automatic Analysis of Elementary Hypotheses

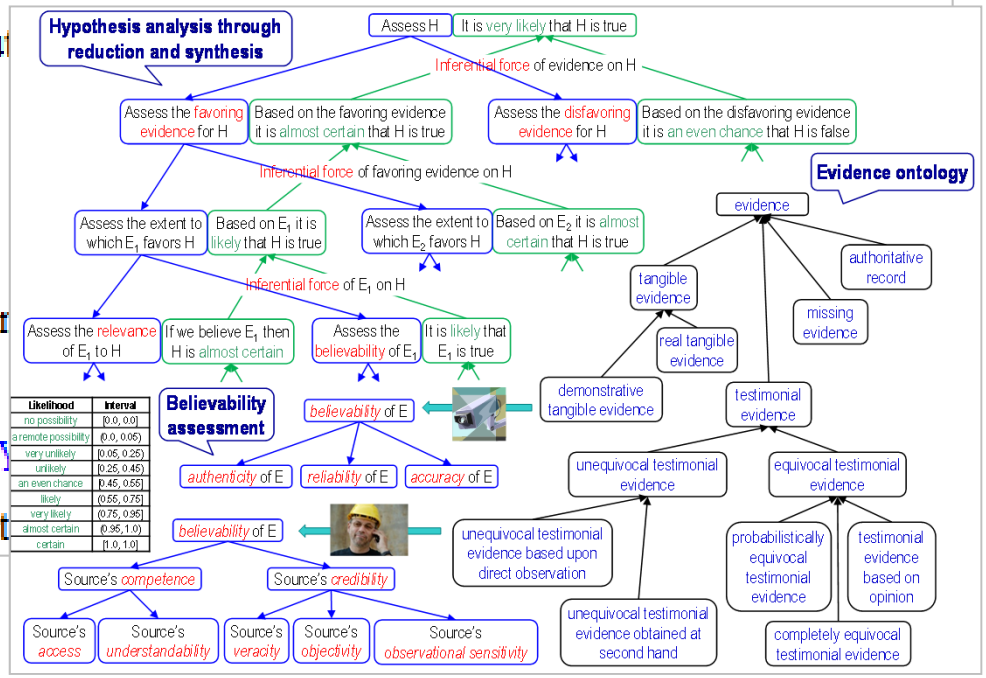


Drill-down Assessment

- Assess whether a cesium-137 canister was stolen from the XYZ warehouse with the MCD-578 truck.: n
  - the cesium-137 canister was in the XYZ warehouse before being reported as missing: almost certain
    - favoring evidence: almost certain
      - EVD-002-Ralph: almost certain
        - relevance: *certain*
        - believability EVD-002-Ralph: almost certain
          - believability Ralph: *almost certain*
            - competence Ralph: no solution
              - access: no solution
              - understandability: no solu
            - credibility Ralph: no solution
              - veracity: no solution
              - objectivity: no solution
              - observational sensitivity: r
    - disfavoring evidence: no solution
  - the cesium-137 canister is no longer in the XY
  - it is true that the cesium-137 canister was not

2. TIACRITIS computes the inferential force on elementary hypotheses

1. Analyst assesses the relevance of evidence and the believability credentials, at the desired level of detail



Hypothesis Testing

Assess whether a cesium-137 canister was stolen from the XYZ warehouse with the MCD-578 truck.

very likely (max)

3. Final result

Q:Which is an assessment strategy?
A:Determine that a cesium-137 canister is missing and that it was stolen with the MCD-578 truck.

very likely (average)

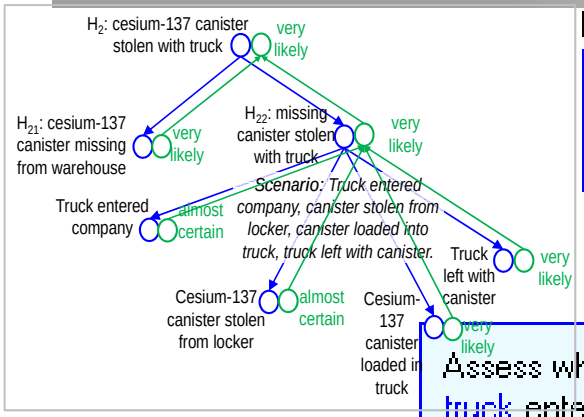
Assess whether a cesium-137 canister is missing from the XYZ warehouse.

very likely (max)

Assess whether the missing cesium-137 canister was stolen wit
the MCD-578 truck.

very likely (max)

2. TIACRITIS computes the inferential force on hypotheses



Q:Which is a possible scenario?
A:The MCD-578 truck entered the XYZ warehouse, the cesium-137 canister was stolen from th
loaded into the truck which left with it.

very likely (min)

1. Analyst selects composition functions (min, max, average, weighted sum)

Assess whether the MCD-578 truck entered the XYZ warehouse.

almost certain (max)

Assess whether the cesium-137 canister was stolen from the hazardous material locker.

almost certain (max)

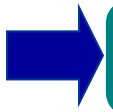
Assess whether the cesi
137 canister was loaded
MCD-578 truck.

very likely (max)

Overview

Computational Theory of Intelligence Analysis

Hypotheses Analysis with TIACRITIS

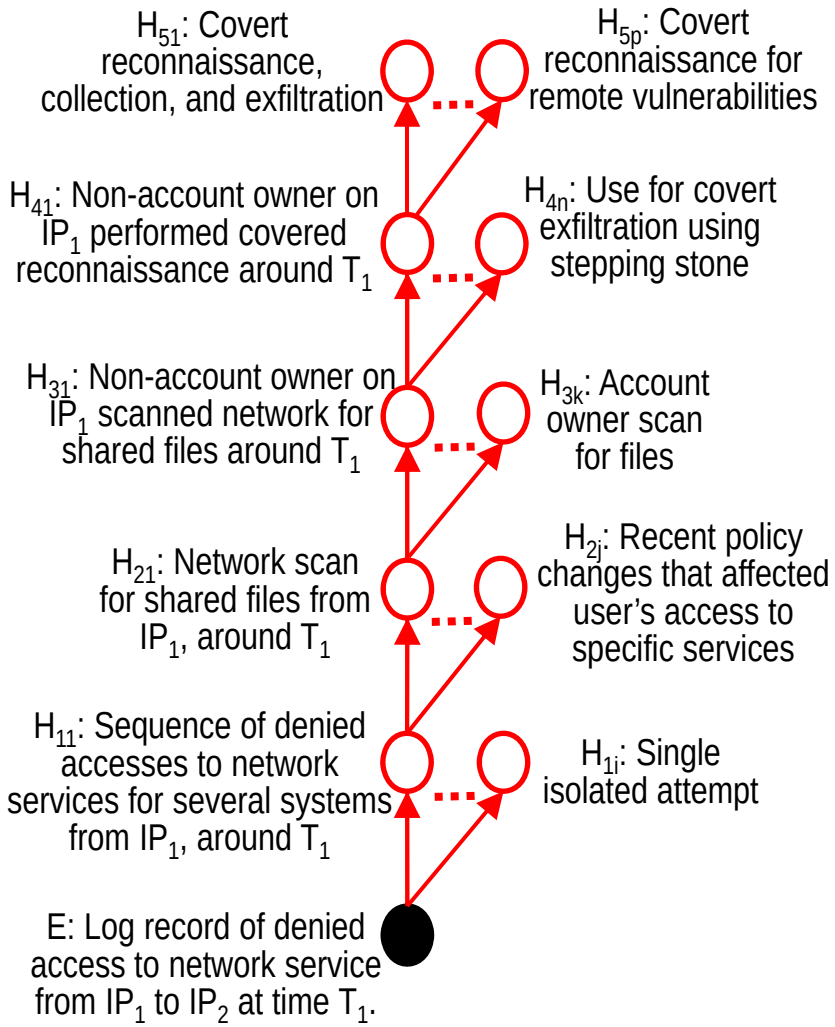


Cyber Insider Threat Discovery and Analysis

Future Research and Development

Discussion

Cyber Insider Threat Discovery and Analysis



Cyber Insider Threats are persons who operate inside an organization and use legitimate access and normal tactics to accomplish abnormal and malicious missions, such as, data reconnaissance, collection and exfiltration, or creating vulnerabilities for attacks by outsiders.

Major national security concern.

Major concern for businesses that need to protect their intellectual property.

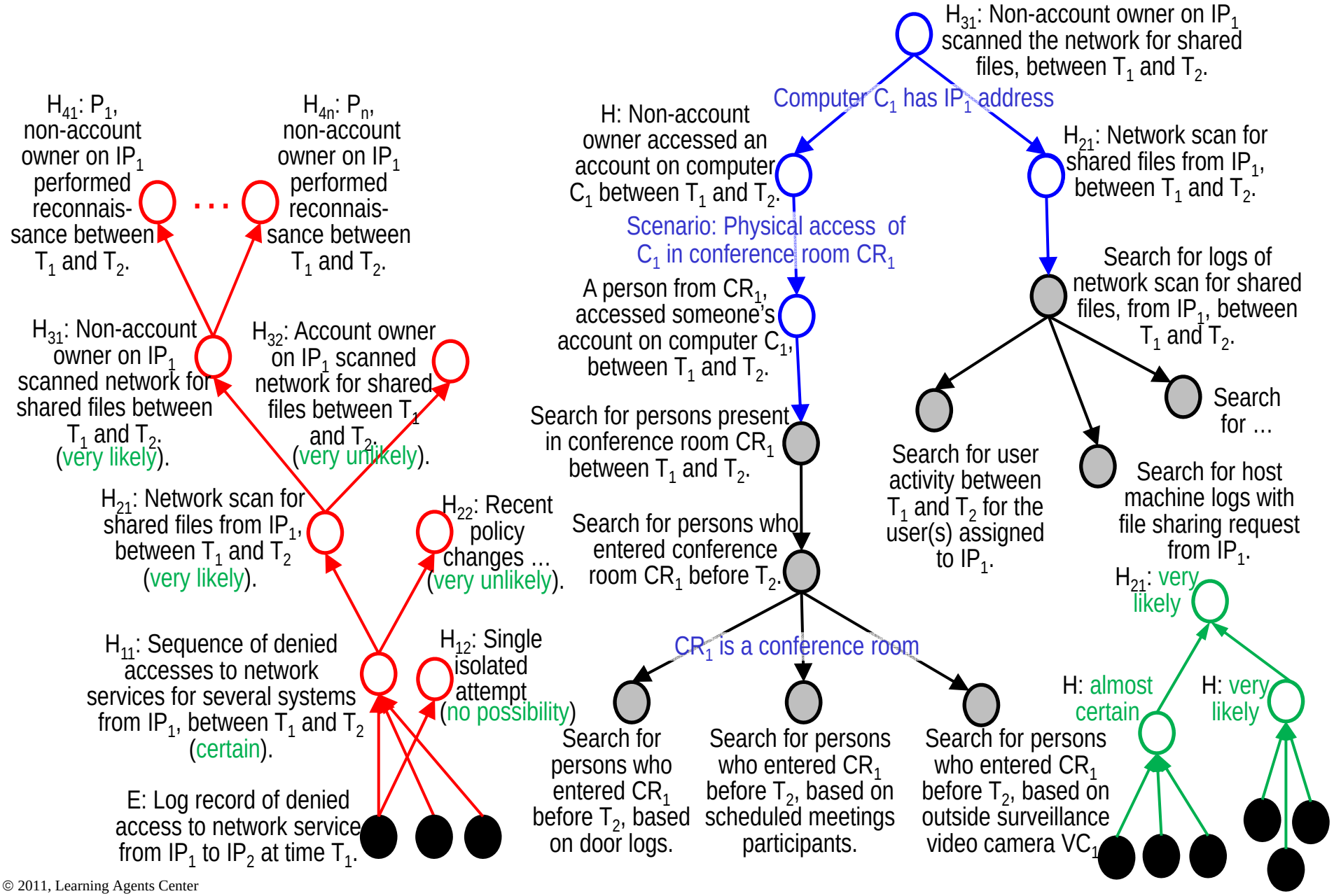
Major privacy concern.

Subject Matter Expert:
Angelos Stavrou

What insider mission might explain this observation?

Abductive reasoning (P → possibly Q)

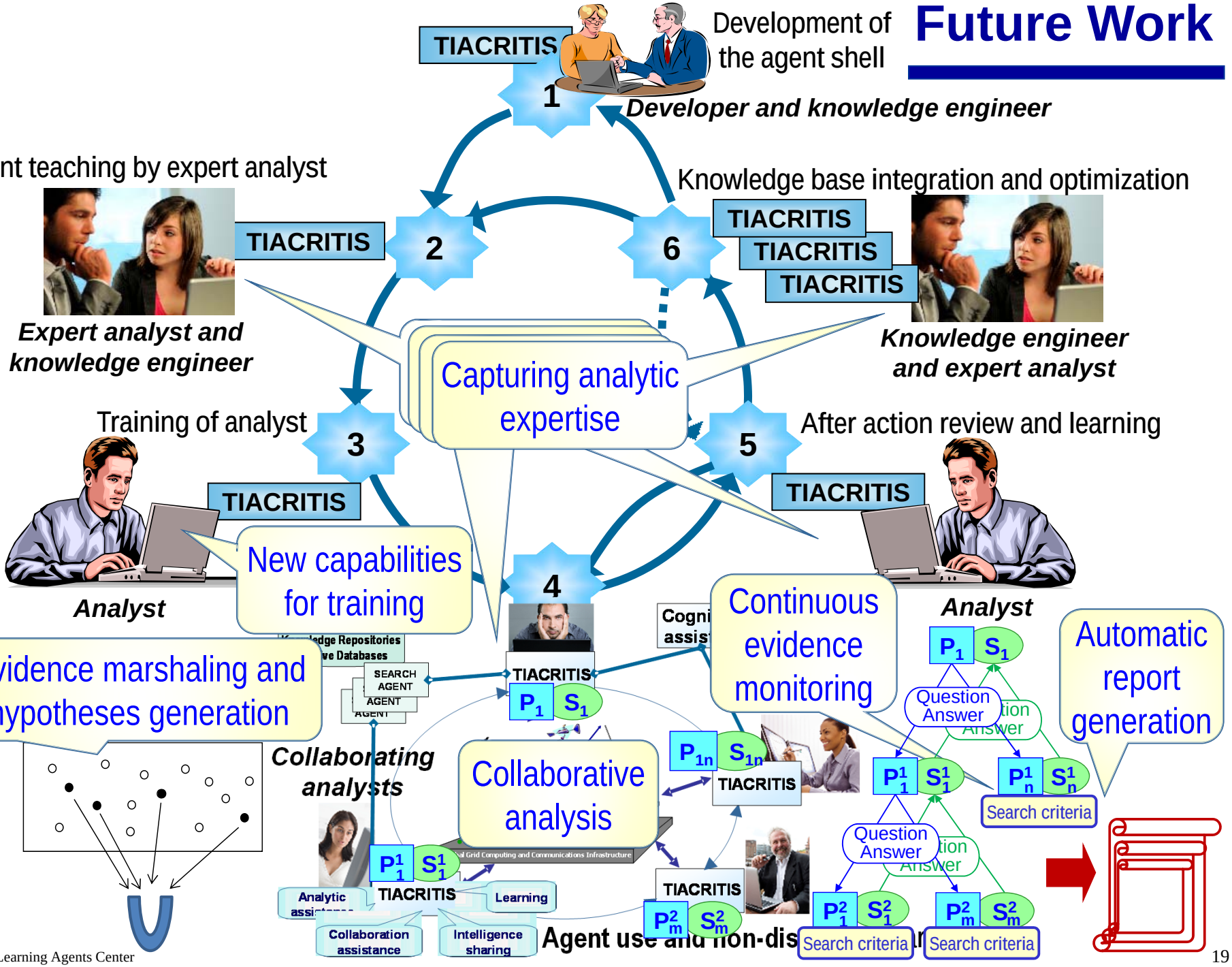
Cyber Insider Threat Discovery and Analysis



Overview

- Computational Theory of Intelligence Analysis
- Hypotheses Analysis with TIACRITIS
- Cyber Insider Threat Discovery and Analysis
- **Future Research and Development**
- Discussion

Future Work



Discussion

Acknowledgements

This research was partially supported by the National Geospatial-Intelligence Agency (PM Phillip Hwang), by the Department of Defense (PMs Erin Gibbens and Benjamin Hamilton), and by George Mason University. It was also guided by the following Advisory Board: Donald Kerr (chair), Kelcy Allwein, Keith Anthony, Cindy Ayers, Sharon Hamilton, Jim Homer, Joan McIntyre, William Nolte, George Stemler, and Benjamin Wible.

The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the U.S. Government.

The U.S. Government is authorized to reproduce and distribute reprints for Government purposes notwithstanding any copyright notation thereon.