INL/CON-23-71120-Revision-1

A Data Processing Pipeline for Adversarial Socio-Technical Network Analysis

June 2023

Gabriel Arthur Weaver, Daniel A. Eisenberg

Changing the World's Energy Future

INL is a U.S. Department of Energy National Laboratory operated by Battelle Energy Alliance, LLC

INL/CON-23-71120-Revision-1

A Data Processing Pipeline for Adversarial Socio-Technical Network Analysis

Gabriel Arthur Weaver, Daniel A. Eisenberg

June 2023

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

A Data Processing Pipeline for Socio-Technical Network Analysis

Battelle Energy Alliance manages INL for the
U.S. Department of Energy's Office of Nuclear Energy

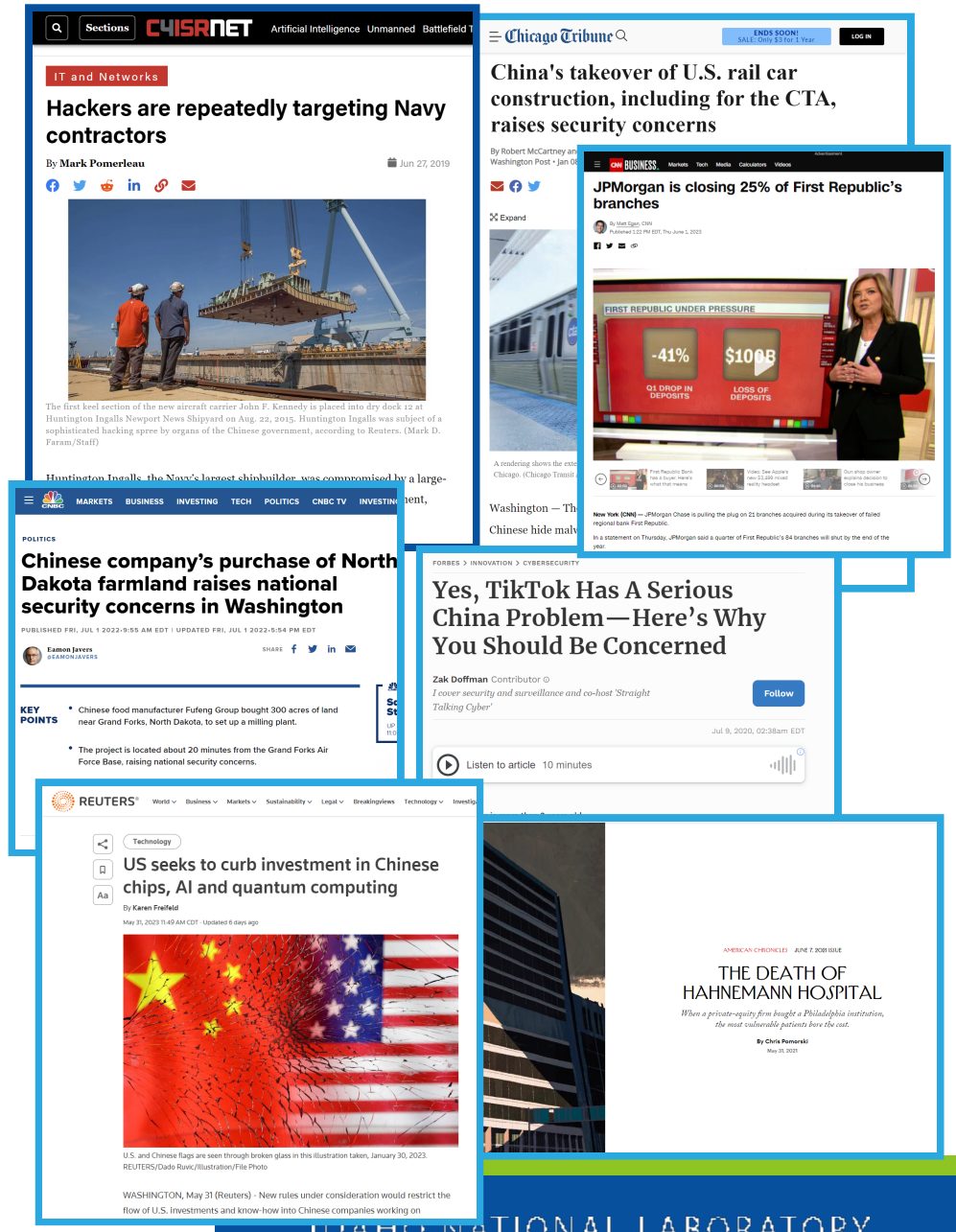
Idaho National Laboratory

Motivation

The Problem: How do adversarial business practices impact critical infrastructure systems within a given geographic region of interest?

Specialization of ‘cyber’ may lead to blindspots for dependencies that achieve influence but are exogenous to traditional system boundaries.

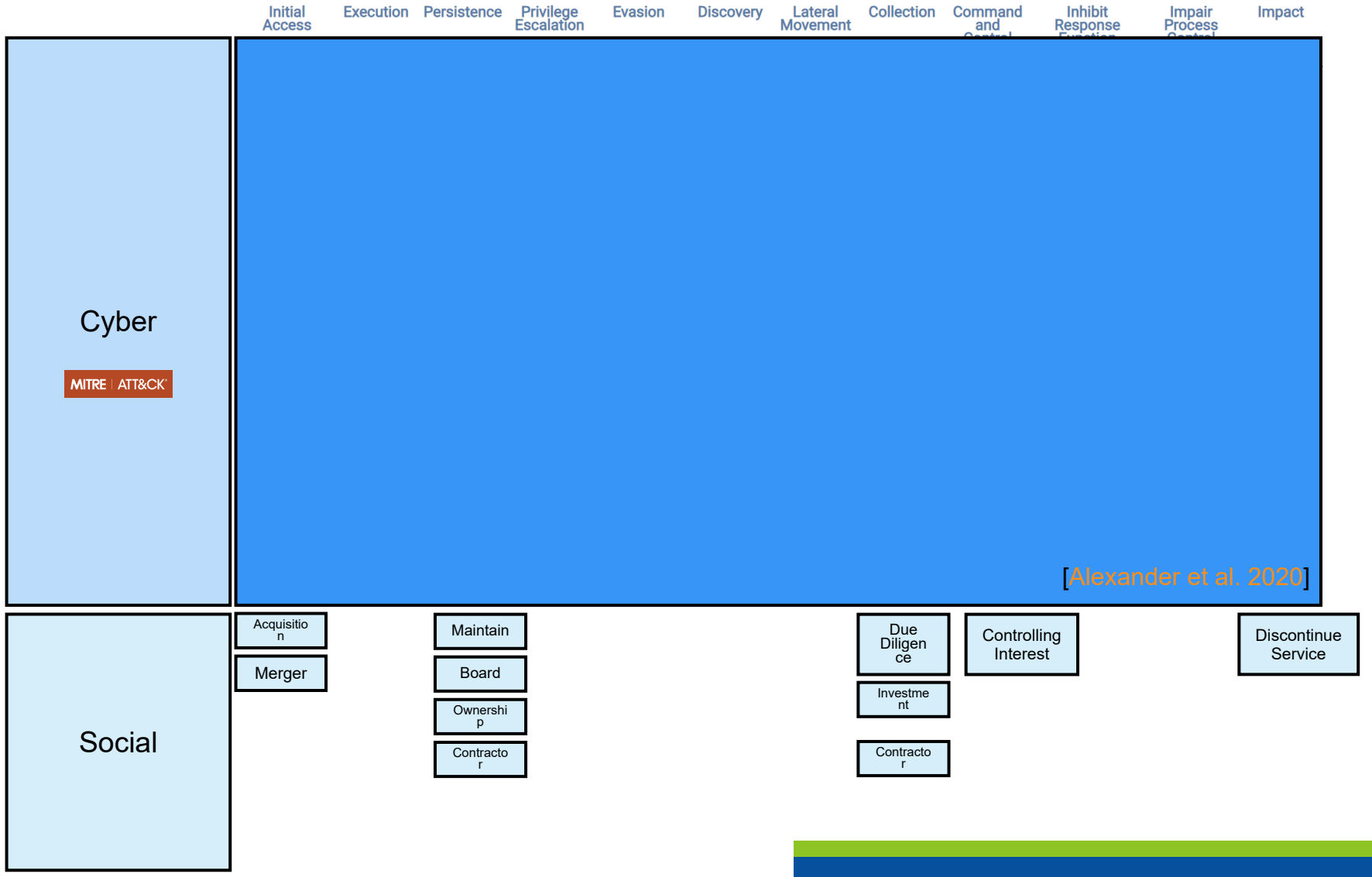
Socio-Technical Network Analysis (STNA) provides an approach to consider interactions between social and cyber domains.



Tactics achieved through the cyber domain may also be achieved through social/business domains.

Our research focuses on adversarial techniques in the business domain that affect infrastructure.

- Want to think about how such techniques across domains can be composed by adversaries.
- Cross-domain 'kill-chains' (e.g. [Assante et al. 2015])

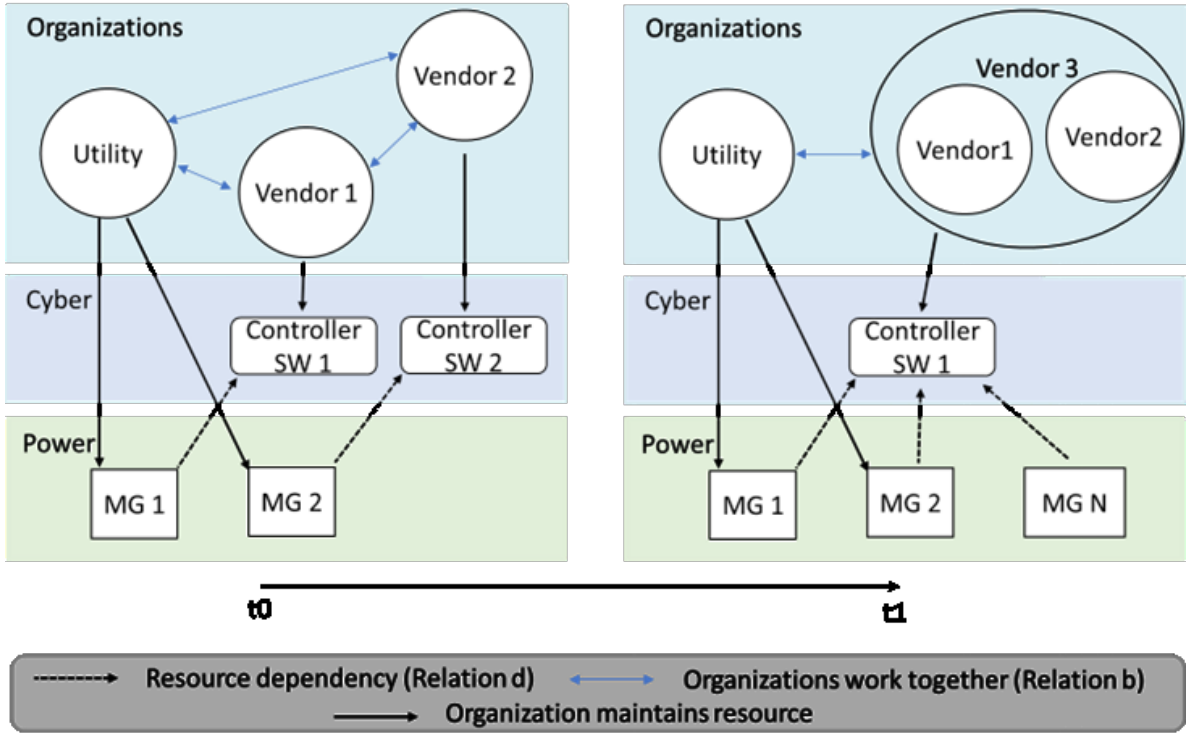


Our Approach: Adversarial STNA

Contributions

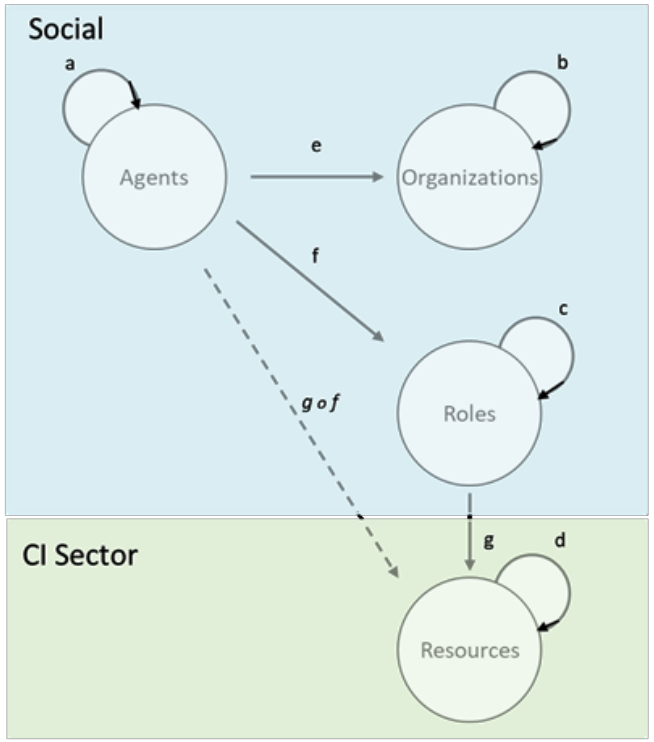
1. Develop a data curation and processing pipeline to generate *Adversarial Socio-Technical Networks (ASTNs)*.

2. Networks produced by our pipeline may be processed as knowledge, geospatial, or dynamic graphs.
   - Enable a variety of analyses to characterize and detect adversarial behaviors



Outline

- Introduction
- ASTN Pipeline Overview
- Use Cases
- Conclusion



Data Sources			
Relation	**Description**	**Data Sources**	**STNA Dynamics**
a	Who knows who?	Emails, call logs	Communications
b	Which organizations work together?	Regional exercises	Information sharing
c	Who reports to whom?	Org chart	Information sharing
d	Which resources depend on each other?	Infrastructure schematics, RRAPs	Infrastructure workflows
e	Who works where?	LinkedIn, Email Address Workflow [32]	Start/end job
f	Who performs what function?	LinkedIn	Maintenance, patching, updates, installation
g	What functions use which resources?	RRAPs, org chart	Access, ownership, acquisition
g o f	Who uses which resources	*Inferred*	Access, ownership, acquisition

ASTN Pipeline Architecture

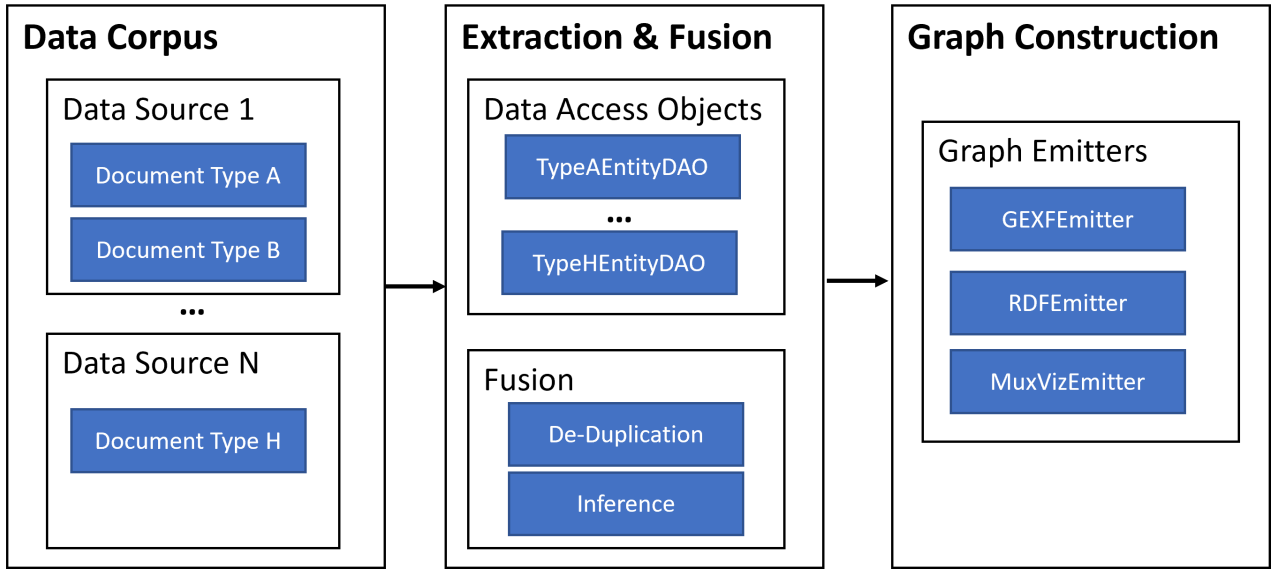
The intent is to construct multilayered networks for adversarial STNA that can be adapted to a wide variety of analyses.

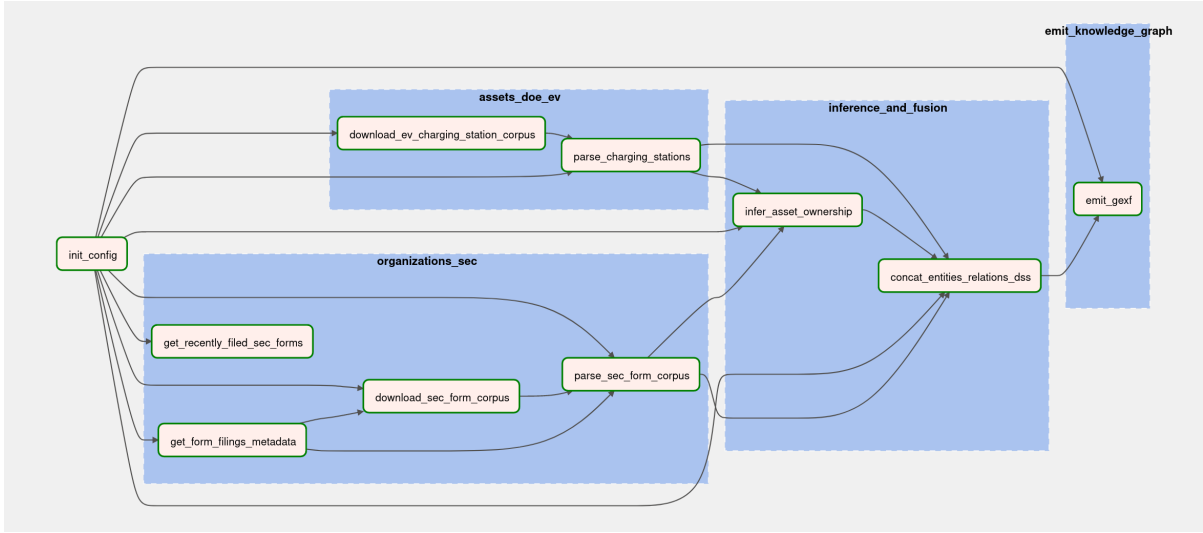
Constructing such networks is difficult

- Diverse, heterogeneous data sources
- Difficult to update, adapt, repurpose

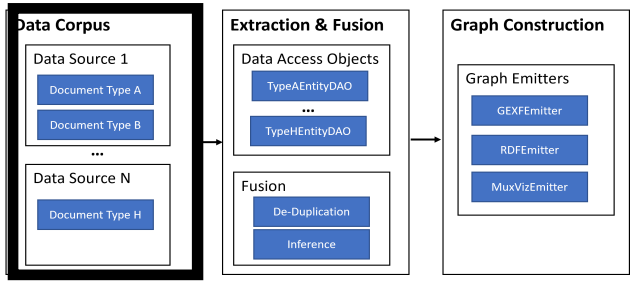
Therefore, we created a data processing pipeline to construct STNA

1. Define types of entities, relations, and attributes via *ontologies*
2. Represent structured relations among entities using *multilayered networks* [Kivela 2014]





Data Corpus



The intent is to construct multilayered networks for adversarial STNA that can be adapted to a wide variety of analyses.

Many types of data sources are available to construct social networks

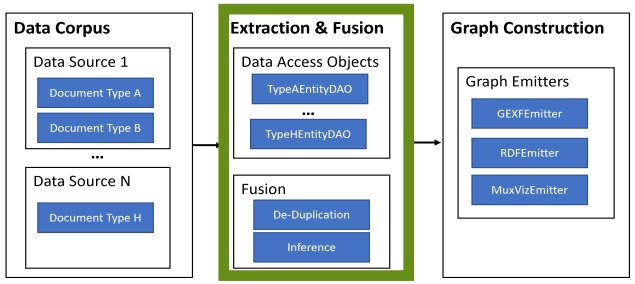
- Twitter [Debreceny 2017]
- Pitchbook, Facebook
- SEC Data [Bichler et al. 2015]

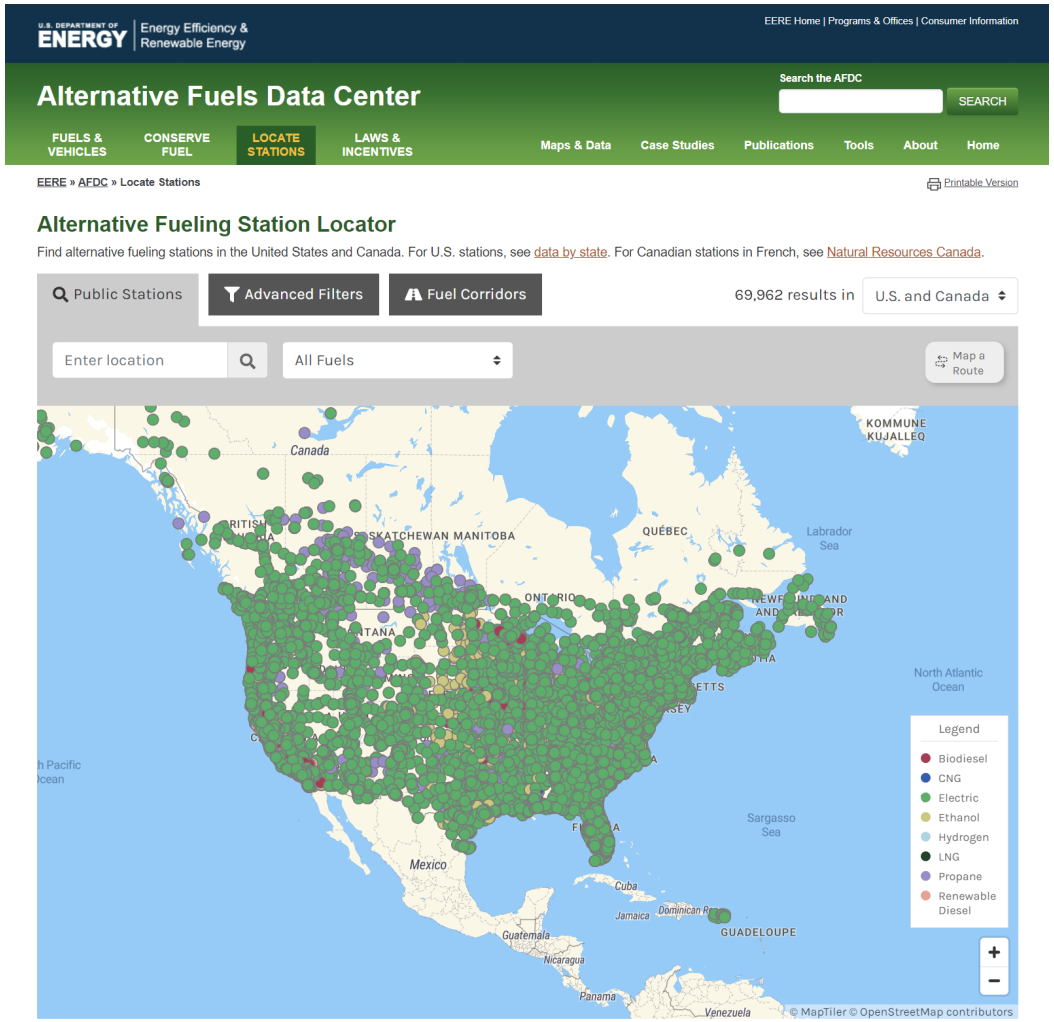
Social Network	
SEC Forms for Organizational Influence	
SEC Form	*Description*
3	Initial statement of beneficial ownership of securities
4	Statement of changes in beneficial ownership
S-4	Registration statement after a merger or acquisition between two companies
SC 13D	Filed when an investor or entity purchases more than 5% shares of a public company.
TO-T	Filed whenever an entity makes a tender offer as part of a takeover bid.

Intent is to be able to

1. Construct the social network layers
2. Compose with layers for a Critical Infrastructure Sector

Critical Infrastructure Sector Entity Extraction



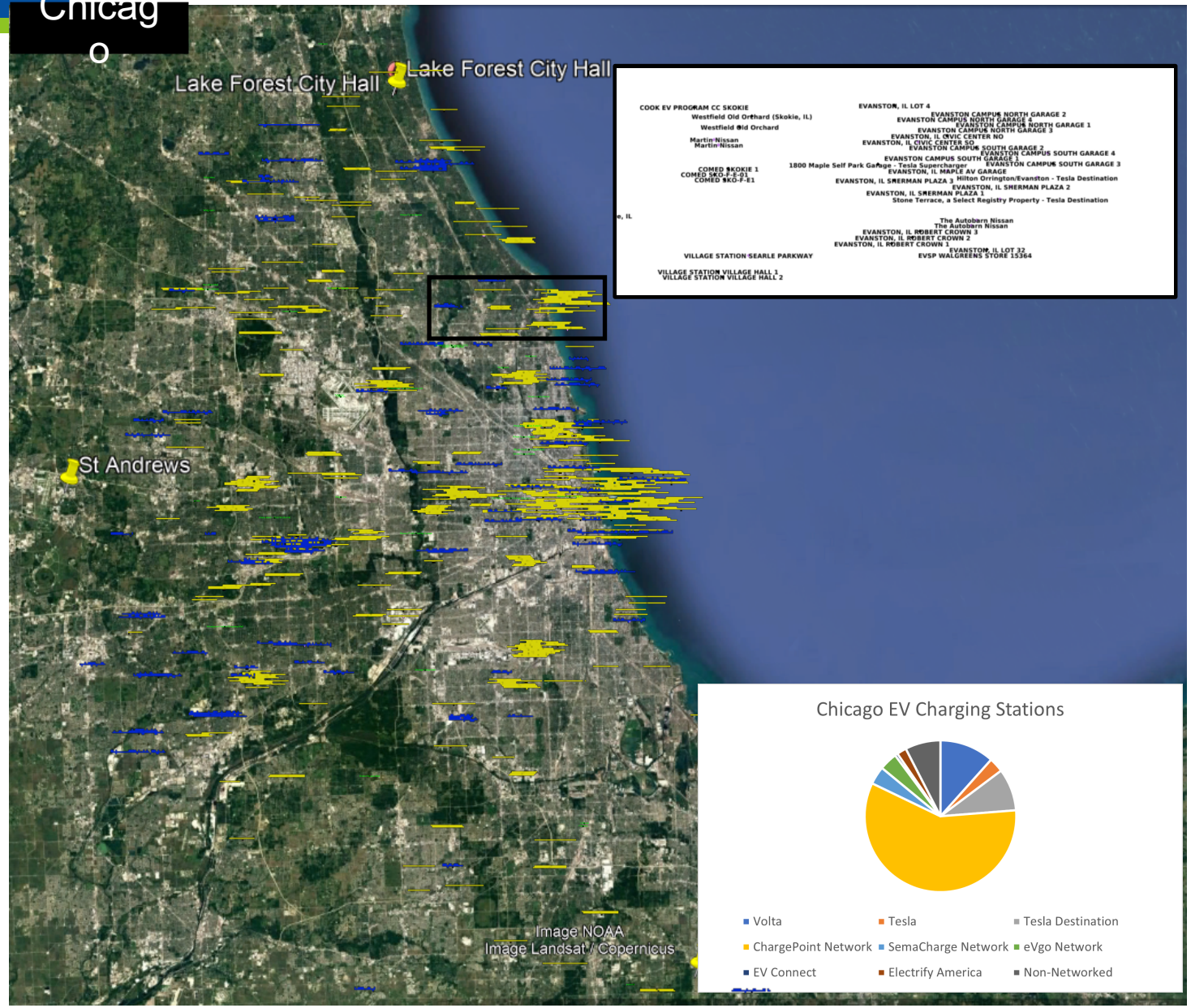


EV Network

alt-fuel-stations.EVChargingStation

hasName	*hasLocation*	*hasEVNetwork*	*Start date*
Paul Simon Chicago JCC	Chicago	Non-Networked	2021-09-21
INTERPARK ADAMWABASH 2	Chicago	ChargePoint Network	2021-12-18
Grant Park South	Chicago	Tesla Destination	2016-02-11

Loss of Availability: Electric Vehicle Charging Station Networks

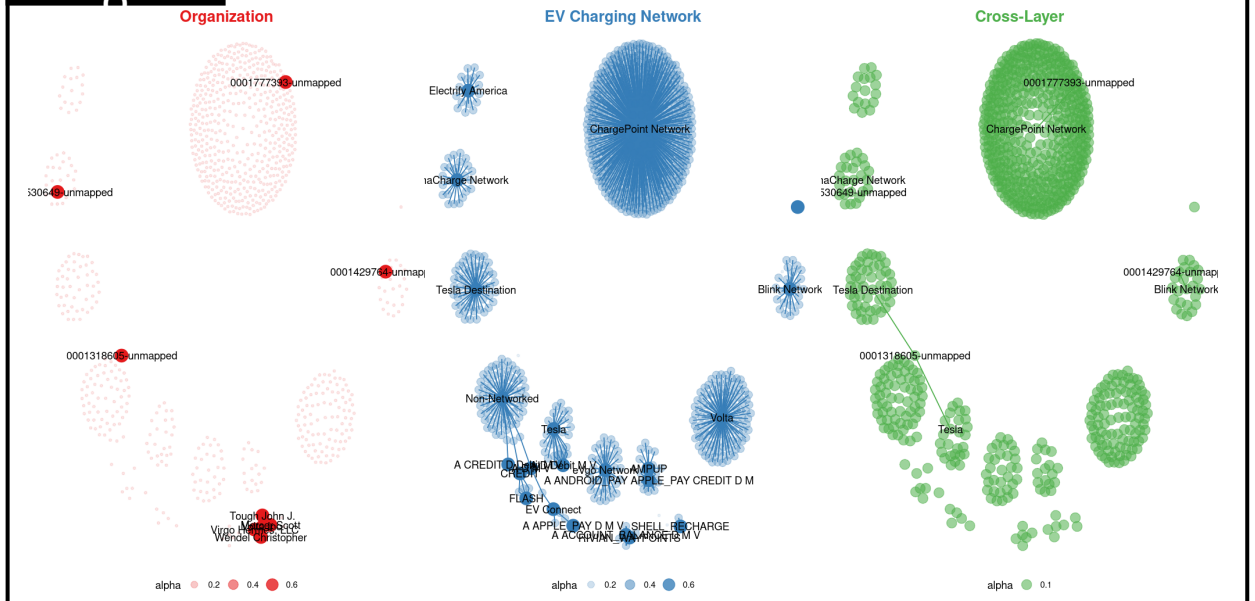


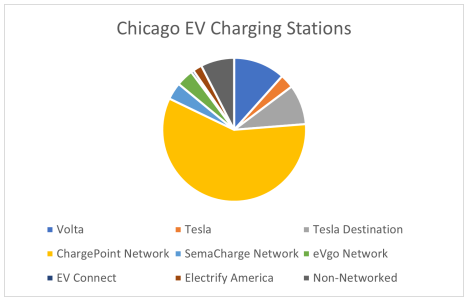
Geospatial Attributes

- Enables the ability to zoom in on a given region of interest and see who has influence and where
  - ChargePoint
  - Volta
  - eVgo
- Data Sources:
  - SEC EDGAR
  - DOE Alt. Fuels Database

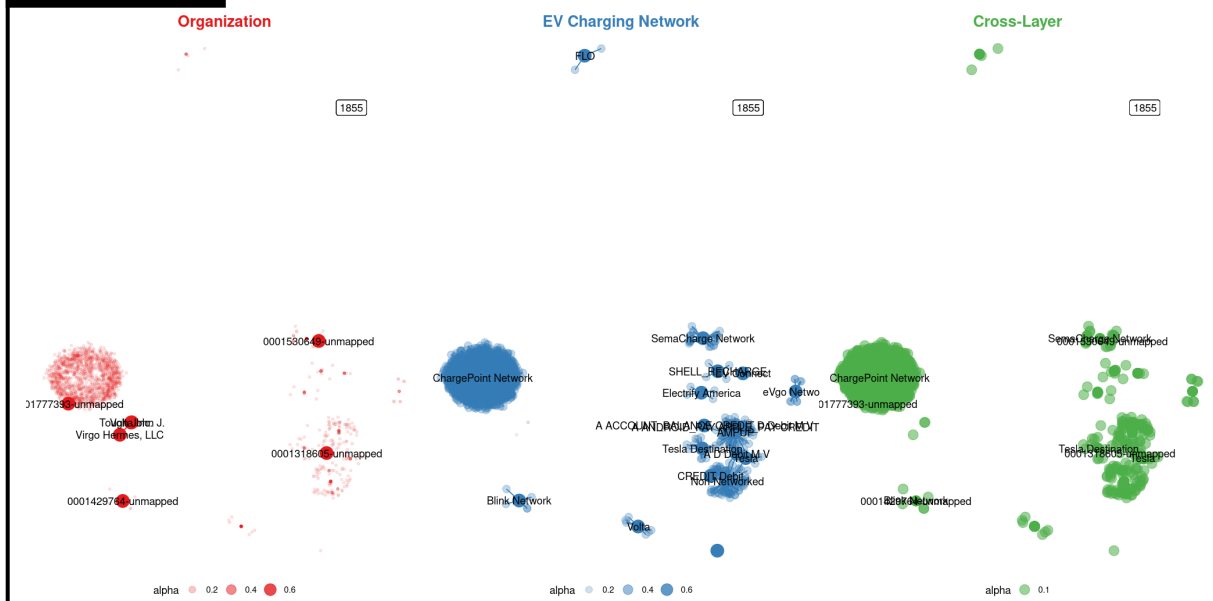
Regional Comparison of EV Charging Station Vendors

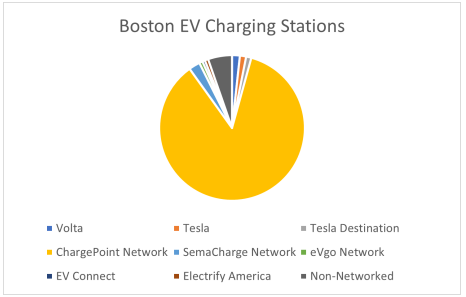
Chicago





Boston





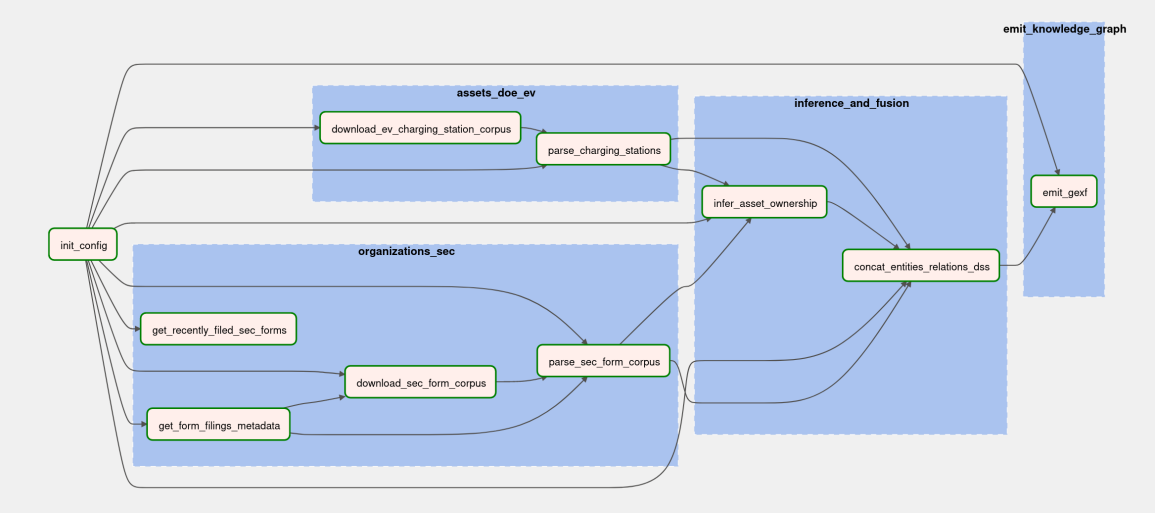
Iterative Discovery

During this analysis of Volta, we discovered the following:

1. Identification of all EV assets within a geographic region of interest.
2. Several other Organizations that own EV Stations in the region.
   - 000177393
   - 0001318605
   - 001429764
   - 0001530649
3. Identification of People/Orgs with a beneficial ownership over Volta
   - CIK: 0001890372
   - CIK: 0001879633

Init Config (n=0)

```
{'edgar.data_dir_path': 'build/chicago/1_23_2023/SEC',
 'evasset.data_dir_path': 'build/chicago/1_23_2023/EVChargingStation',
 'fusion.data_dir_path': 'build/chicago/1_23_2023/fusion',
 'editorial.data_dir_path': './build/chicago/1_23_2023/editorial',
 'edgar.cik_list': ['0001819584'],
 'edgar.form_types': ['SC 13D', 'S-4'],
 'evasset.latitude': '41.8781',
 'evasset.longitude': '-87.6298',
 'evasset.radius': '30.0'}
```



Init Config (n=1)

```
{'edgar.data_dir_path': 'build/chicago/1_23_2023/SEC',
 'edgar.max_cik_form_types_downloaded': 10,
 'evasset.data_dir_path': 'build/chicago/1_23_2023/EVChargingStation',
 'fusion.data_dir_path': 'build/chicago/1_23_2023/fusion',
 'editorial.data_dir_path': './build/chicago/1_23_2023/editorial',
 'edgar.cik_list': ['0001819584',
  '0001777393',
  '0001318605',
  '0001429764',
  '0001530649'],
 'edgar.form_types': ['SC 13D', 'S-4'],
 'evasset.latitude': '41.8781',
 'evasset.longitude': '-87.6298',
 'evasset.radius': '30.0'}
```

Conclusions

The Problem: There is a practical need to be able to analyze sociotechnical dependencies and their evolving risks.

Specialization of ‘cyber’ may lead to blindspots for dependencies that achieve influence but are exogenous to traditional system boundaries.

Our Approach: Our research focuses on adversarial techniques in the business domain that affect critical infrastructure.

Time	Event	Relevance
August 13, 2018	Foreign Investment Risk Review Modernization Act (FIRRMA)	CFIUS has increased jurisdiction over investments in US businesses that afford a foreign person the following: • Access to material nonpublic technical information • Membership or observer rights on, or the right to nominate an individual to a position on a board • Involvement, other than through voting in decision making of US business for critical technology
May 31, 2023	US Treasury considering export controls	• New rules would restrict flow of U.S. investments into Chinese companies working in advanced semiconductors, AI, and quantum.

Idaho National Laboratory

Battelle Energy Alliance manages INL for the U.S. Department of Energy's Office of Nuclear Energy. INL is the nation's center for nuclear energy research and development, and also performs research in each of DOE's strategic goal areas: energy, national security, science and the environment.

Overflow

Newport News Shipping

Historical Study, Indirect Data Access via Subsidiary

Sections C4ISRNET Artificial Intelligence Unmanned Battlefield Tech Space Electronic Warfare Cyber

IT and Networks

Hackers are repeatedly targeting Navy contractors

By **Mark Pomerleau** Jun 27, 2019

The first keel section of the new aircraft carrier John F. Kennedy is placed into dry dock 12 at Huntington Ingalls Newport News Shipyard on Aug. 22, 2015. Huntington Ingalls was subject of a sophisticated hacking spree by organs of the Chinese government, according to Reuters. (Mark D. Faram/Staff)

Huntington Ingalls, the Navy's largest shipbuilder, was compromised by a large-scale hacking campaign waged by several organs of the Chinese government, according to a Reuters report.

However, the company denied the allegation in a June 27 email to Fifth Domain, saying, "there was no breach of information" from Newport News Shipyard, nor were their systems connected to a foreign server controlled by a Chinese group, known as APT10.

Featured Video

NAVY FEDERAL Credit Union

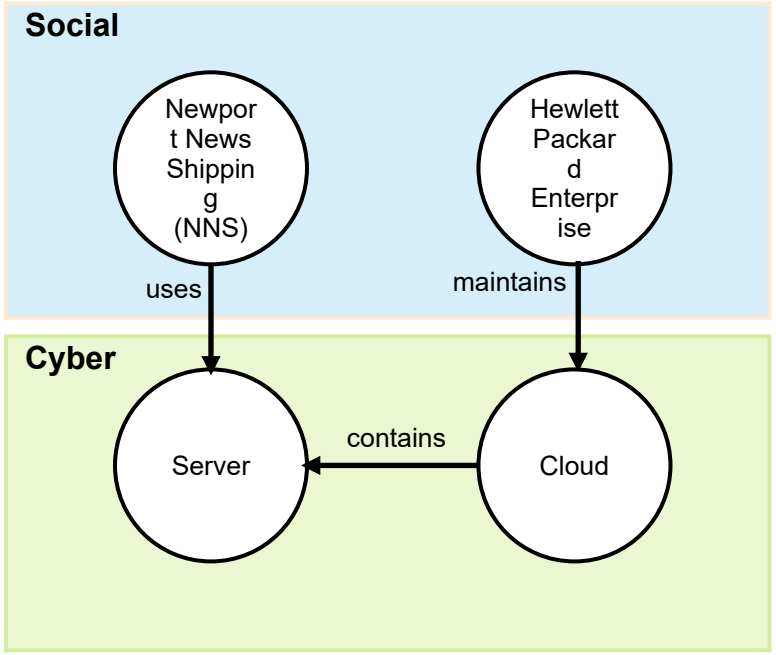
Electric tanks and upgraded targeting drones | Defense News Weekly Full Episode 10.22.22

This smart shirt might save your life on the battlefield

The importance of rigorous testing

Future Tactical UAS offerings at AUSA

Newport News Shipping Case Study



Construction of G_1:

1. NNS uses a Server
2. Cloud contains Server
3. HPE/CSC maintains Cloud

Time:

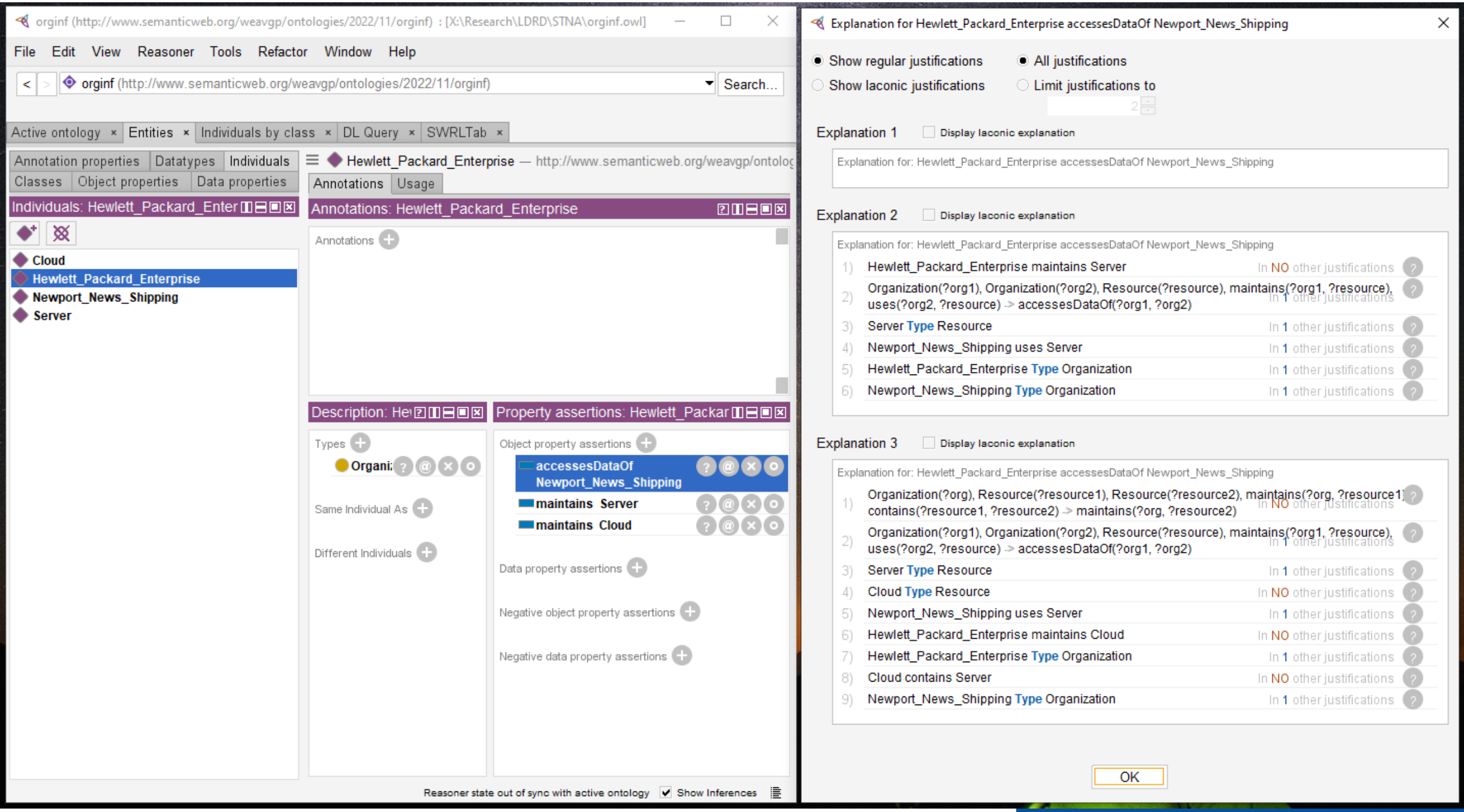
From time t1_1 to time t2_1.

Inference:

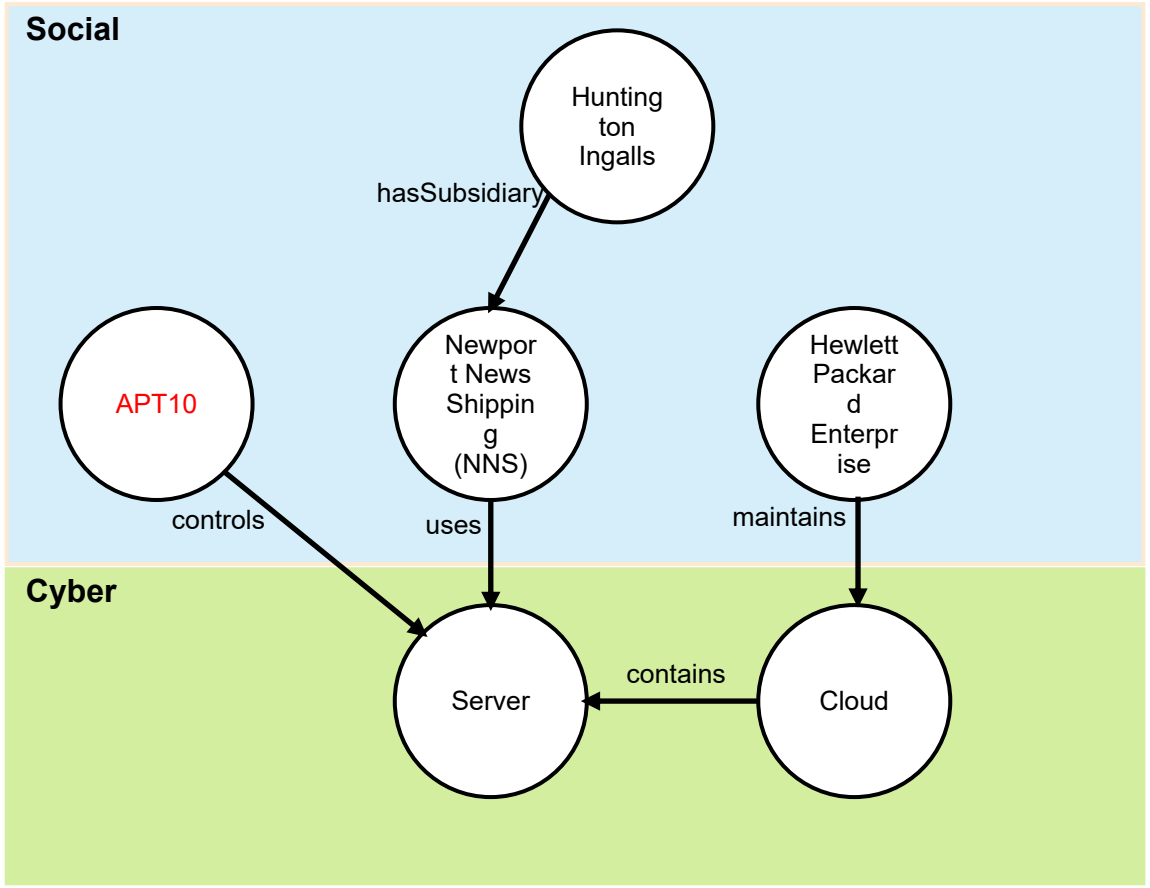
1. <org1> maintains <resource1> & <resource1> contains <resource2> → <org1> maintains <resource2>
2. <org1> maintains <resource2> & <org2> uses <resource2> □ <org1> accessesDataOf <org2>

Relations Inferred:

- HPE maintains Server [I1]
- HPE accessesDataOf NNS [I2]


orginf (http://www.semanticweb.org/weavgp/ontologies/2022/11/orginf) : [X:\Research\LDRD\STNA\orginf.owl]
File Edit View Reasoner Tools Refactor Window Help
orginf (http://www.semanticweb.org/weavgp/ontologies/2022/11/orginf)
Search...
Active ontology × Entities × Individuals by class × DL Query × SWRLTab ×
Annotation properties Datatypes Individuals
Classes Object properties Data properties
Individuals: Hewlett_Packard_Enter
Cloud
Hewlett_Packard_Enterprise
Newport_News_Shipping
Server
Hewlett_Packard_Enterprise — http://www.semanticweb.org/weavgp/ontolog
Annotations Usage
Annotations: Hewlett_Packard_Enterprise
Annotations
Description: He
Types
Organi
Same Individual As
Different Individuals
Property assertions: Hewlett_Packar
Object property assertions
accessesDataOf Newport_News_Shipping
maintains Server
maintains Cloud
Data property assertions
Negative object property assertions
Negative data property assertions
Reasoner state out of sync with active ontology
Show Inferences
Explanation for Hewlett_Packard_Enterprise accessesDataOf Newport_News_Shipping
Show regular justifications
All justifications
Show laconic justifications
Limit justifications to
2
Explanation 1
Display laconic explanation
Explanation for: Hewlett_Packard_Enterprise accessesDataOf Newport_News_Shipping
Explanation 2
Display laconic explanation
Explanation for: Hewlett_Packard_Enterprise accessesDataOf Newport_News_Shipping
1) Hewlett_Packard_Enterprise maintains Server — In NO other justifications
2) Organization(?org1), Organization(?org2), Resource(?resource), maintains(?org1, ?resource), uses(?org2, ?resource) -> accessesDataOf(?org1, ?org2) — In 1 other justifications
3) Server Type Resource — In 1 other justifications
4) Newport_News_Shipping uses Server — In 1 other justifications
5) Hewlett_Packard_Enterprise Type Organization — In 1 other justifications
6) Newport_News_Shipping Type Organization — In 1 other justifications
Explanation 3
Display laconic explanation
Explanation for: Hewlett_Packard_Enterprise accessesDataOf Newport_News_Shipping
1) Organization(?org), Resource(?resource1), Resource(?resource2), maintains(?org, ?resource1), contains(?resource1, ?resource2) -> maintains(?org, ?resource2) — In NO other justifications
2) Organization(?org1), Organization(?org2), Resource(?resource), maintains(?org1, ?resource), uses(?org2, ?resource) -> accessesDataOf(?org1, ?org2) — In 1 other justifications
3) Server Type Resource — In 1 other justifications
4) Cloud Type Resource — In NO other justifications
5) Newport_News_Shipping uses Server — In 1 other justifications
6) Hewlett_Packard_Enterprise maintains Cloud — In NO other justifications
7) Hewlett_Packard_Enterprise Type Organization — In 1 other justifications
8) Cloud contains Server — In NO other justifications
9) Newport_News_Shipping Type Organization — In 1 other justifications
OK

Upstream Impacts via Social Network Analysis



Inference Rules:

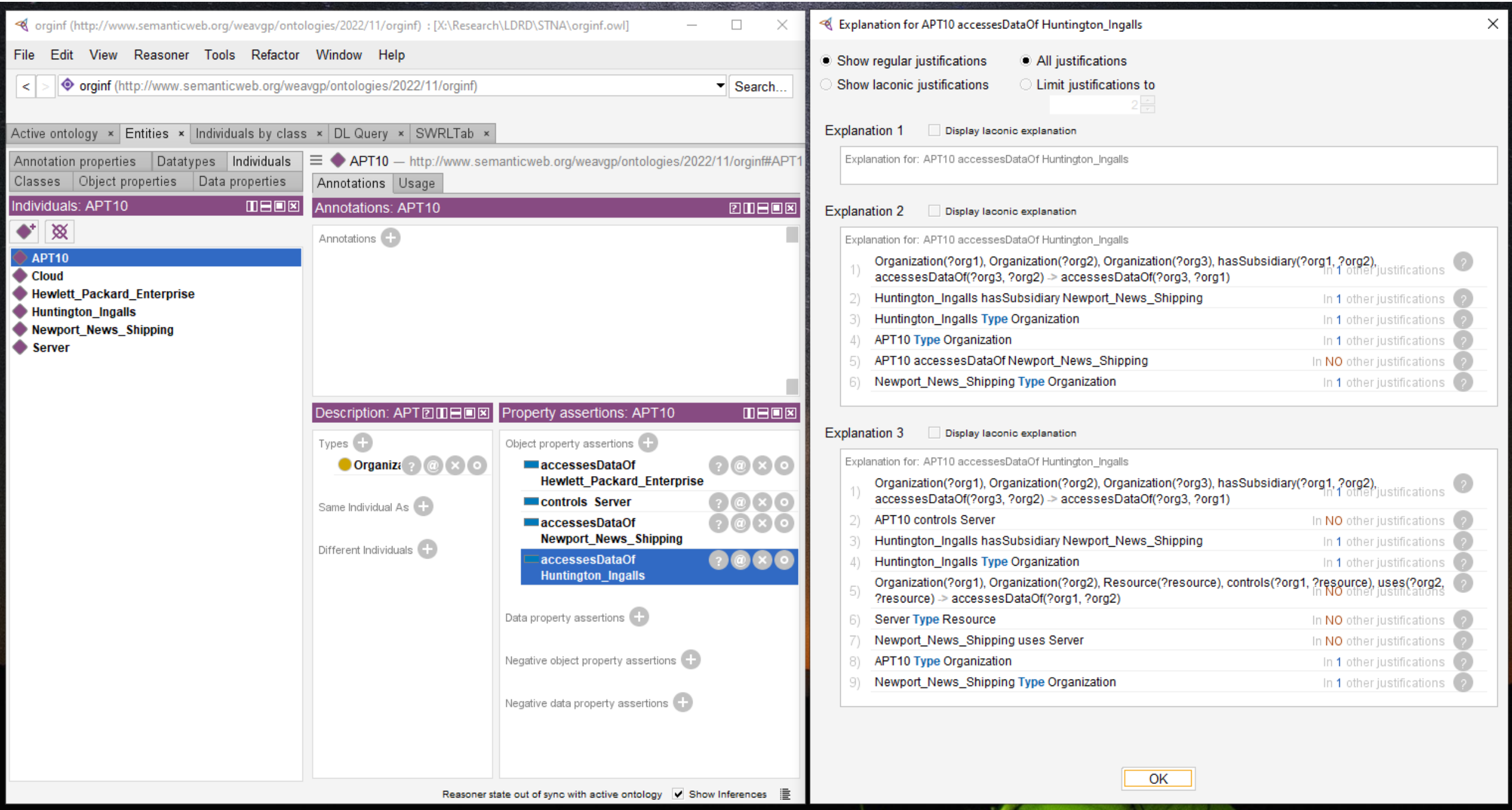
1. <org1> maintains <resource1> & <resource1> contains <resource2> → <org1> maintains <resource2>
2. <org1> maintains <resource2> & <org2> uses <resource2> □ <org1> accessesDataOf <org2>
3. <org1> controls <resource2> & <org2> uses <resource2> □ <org1> accessesDataOf <org2>
4. <org1> controls <resource2> & <org2> maintains <resource2> □ <org1> accessesDataOf <org2>
5. <org3> hasSubsidiary <org2> & <org1> accessesDataOf <org2> □ <org1> accessesDataOf <org3>

Data Sets:

- hasSubsidiary via OpenCorporates (?)

Inferred Relations

- HPE maintains Server [I1]
- HPE accessesDataOf NNS [I2]
- APT10 accessesData of NNS [I3]
- APT10 accessesData of HPE [I4]
- APT10 accessesData of HuntingtonIngalls [I5]


orginf (http://www.semanticweb.org/weavgp/ontologies/2022/11/orginf) : [X:\Research\LDRD\STNA\orginf.owl]
File Edit View Reasoner Tools Refactor Window Help
orginf (http://www.semanticweb.org/weavgp/ontologies/2022/11/orginf)
Search...
Active ontology × Entities × Individuals by class × DL Query × SWRLTab ×
Annotation properties Datatypes Individuals
Classes Object properties Data properties
Individuals: APT10
APT10
Cloud
Hewlett_Packard_Enterprise
Huntington_Ingalls
Newport_News_Shipping
Server
APT10 — http://www.semanticweb.org/weavgp/ontologies/2022/11/orginf#APT1
Annotations Usage
Annotations: APT10
Annotations
Description: APT
Types
Organiza
Same Individual As
Different Individuals
Property assertions: APT10
Object property assertions
accessesDataOf Hewlett_Packard_Enterprise
controls Server
accessesDataOf Newport_News_Shipping
accessesDataOf Huntington_Ingalls
Data property assertions
Negative object property assertions
Negative data property assertions
Reasoner state out of sync with active ontology
Show Inferences
Explanation for APT10 accessesDataOf Huntington_Ingalls
Show regular justifications
All justifications
Show laconic justifications
Limit justifications to
2
Explanation 1
Display laconic explanation
Explanation for: APT10 accessesDataOf Huntington_Ingalls
Explanation 2
Display laconic explanation
Explanation for: APT10 accessesDataOf Huntington_Ingalls
1) Organization(?org1), Organization(?org2), Organization(?org3), hasSubsidiary(?org1, ?org2), accessesDataOf(?org3, ?org2) -> accessesDataOf(?org3, ?org1) In 1 other justifications
2) Huntington_Ingalls hasSubsidiary Newport_News_Shipping In 1 other justifications
3) Huntington_Ingalls Type Organization In 1 other justifications
4) APT10 Type Organization In 1 other justifications
5) APT10 accessesDataOf Newport_News_Shipping In NO other justifications
6) Newport_News_Shipping Type Organization In 1 other justifications
Explanation 3
Display laconic explanation
Explanation for: APT10 accessesDataOf Huntington_Ingalls
1) Organization(?org1), Organization(?org2), Organization(?org3), hasSubsidiary(?org1, ?org2), accessesDataOf(?org3, ?org2) -> accessesDataOf(?org3, ?org1) In 1 other justifications
2) APT10 controls Server In NO other justifications
3) Huntington_Ingalls hasSubsidiary Newport_News_Shipping In 1 other justifications
4) Huntington_Ingalls Type Organization In 1 other justifications
5) Organization(?org1), Organization(?org2), Resource(?resource), controls(?org1, ?resource), uses(?org2, ?resource) -> accessesDataOf(?org1, ?org2) In NO other justifications
6) Server Type Resource In NO other justifications
7) Newport_News_Shipping uses Server In NO other justifications
8) APT10 Type Organization In 1 other justifications
9) Newport_News_Shipping Type Organization In 1 other justifications
OK

Idaho National Laboratory

Battelle Energy Alliance manages INL for the U.S. Department of Energy's Office of Nuclear Energy. INL is the nation's center for nuclear energy research and development, and also performs research in each of DOE's strategic goal areas: energy, national security, science and the environment.