INL/MIS-23-72124-Revision-1

A Data Processing Pipeline for Socio-Technical Network Analysis

May 2023

Gabriel Arthur Weaver, Daniel

Changing the World's Energy Future

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

INL/MIS-23-72124-Revision-1

A Data Processing Pipeline for Socio-Technical Network Analysis

Gabriel Arthur Weaver, Daniel

May 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

INCOSE WG

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.

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

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

Adversarial tactics seen in the cybersecurity domain may also be achieved through other 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 adversarial kill-chains (inspired by Cyber Kill Chain [Assante et al. 2015])

Social	Acquisition	Ownership	Company Ownership Proxy	Due Diligence for Mergers & Acquisitions	Ownership of Nearby Asset	Parent Company	Foreign-Owned Facilities
	Use	Board Membership	Board Membership Proxy	Legal Subpoena	Pilot Studies		Disinformation
	Leasing	Asset Maintenance		Digital Twin Creation	Business Data Availability Platform Capture		Degrade Service Quality
	Employment	Subcontract/ Supporting Vendor					
		Investing or Lending					
Cyber	Drive-by Compromise	Hardcoded Credentials	Change Operating Mode	Network Connection Enumeration	Data from Information Repositories	Commonly Used Port	Unauthorized Command Message

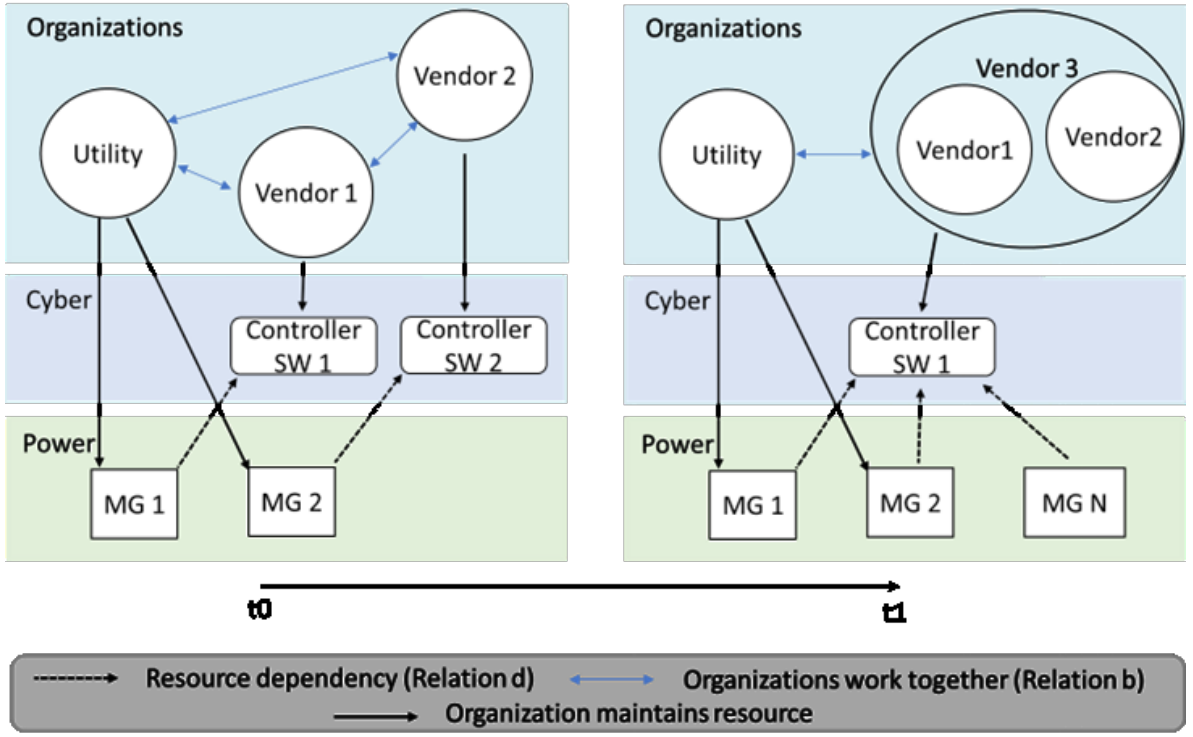
[Alexander et al. 2020]

Our Approach: Adversarial STNA

Contributions

1. Develop a data curation and processing pipeline to generate networks that enable *Adversarial Socio-Technical Network Analysis*.

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

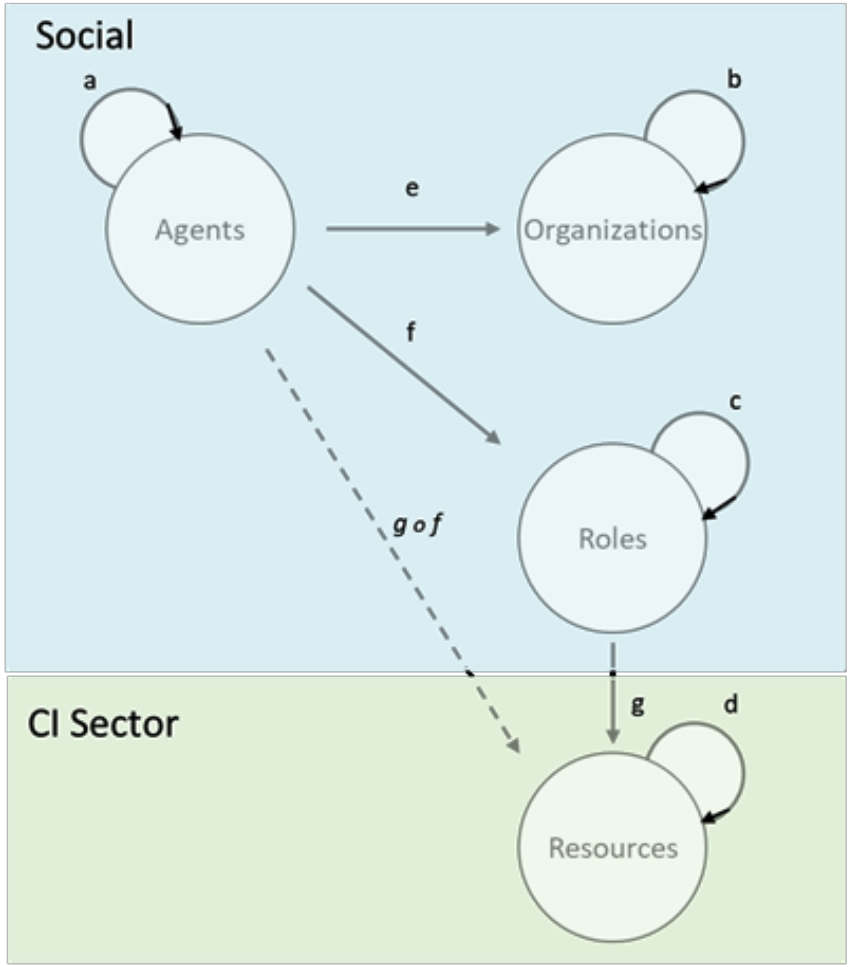
- Introduction
- Theory
- Architecture
- Use Cases
- Conclusion

Theory

Multilayered Networks for Adversarial STNA

Want a systematic approach to study structured relations between domains that can influence critical infrastructure systems (e.g. cyber, social).

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



Network Construction: Entity Occurrences as Vertices

Ontology

- Classes define *entity types*
- Data properties define *attributes* of entities.

Multilayered Network

- Entity types provide values for STNA network's semantic layer.
- Attributes affect vertex weighting functions

Social Network: Entity Types and Data Properties			
Entity Type	***Data Property***	***Description***	***Network Component***
stna_core.Organization	hasCIK	Central Index Key (CIK)	V
	hasSIC	Standard Industrial Classification (SIC)	w_semantic
	hasBusinessAddress	Business address	L_Geospatial
	hasStateOfIncorporation	State of Incorporation	L_Geospatial
stna_core.Person	hasConformedName	Conformed Name	V
	hasOfficerTitle	Officer title	w_semantic
	hasBusinessAddress	Business Address	L_Geospatial

Network Construction: Relations as Edges

Ontology

Object properties define *relations* between entities.

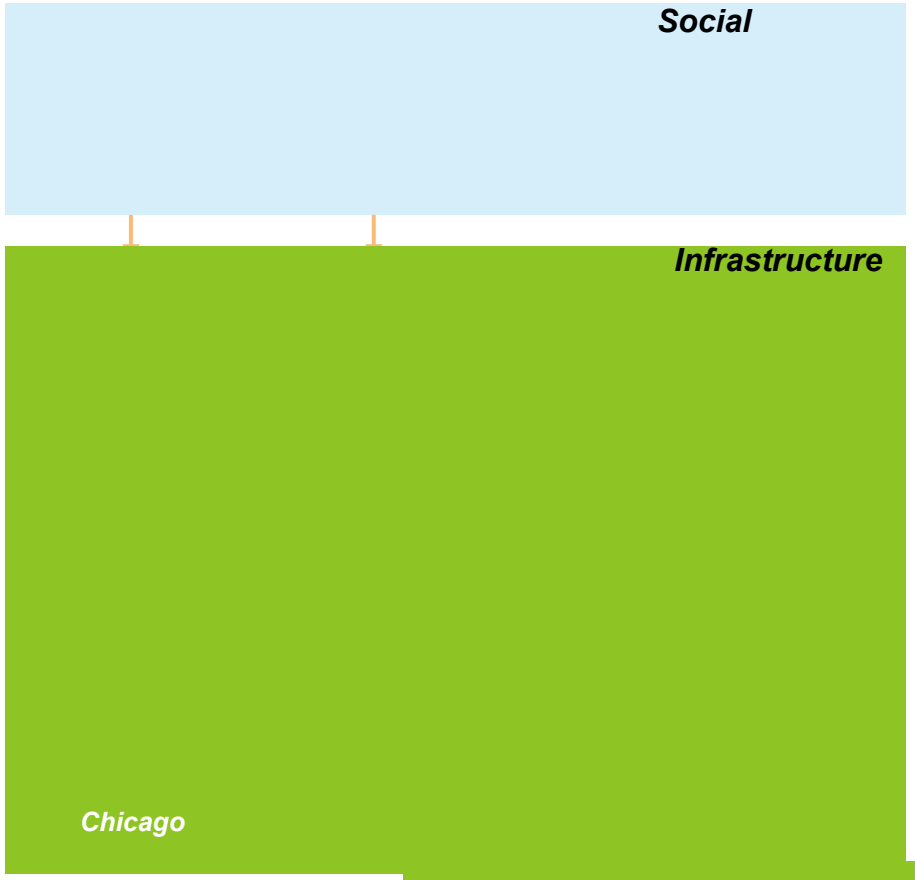
Object Properties and Features to Construct EM		
Object Property	***Subject Class***	***Object Class***
Social Network		
`hasBeneficialOwnership`	Organization Person	Organization

`isDirectorOf`
`isOfficerOf`
`isTenPercentOwnerOf`
	Person	Organization

Infrastructure Network		
`hasEVNetwork`	EVChargingStation	EVChargingNetwork
`hasPaymentNetwork`	EVChargingStation	PaymentNetwork
Inter-Layer (Socio-Technical)		
`owns` `maintains`	Organization Person	CIAsset

Multilayered Network

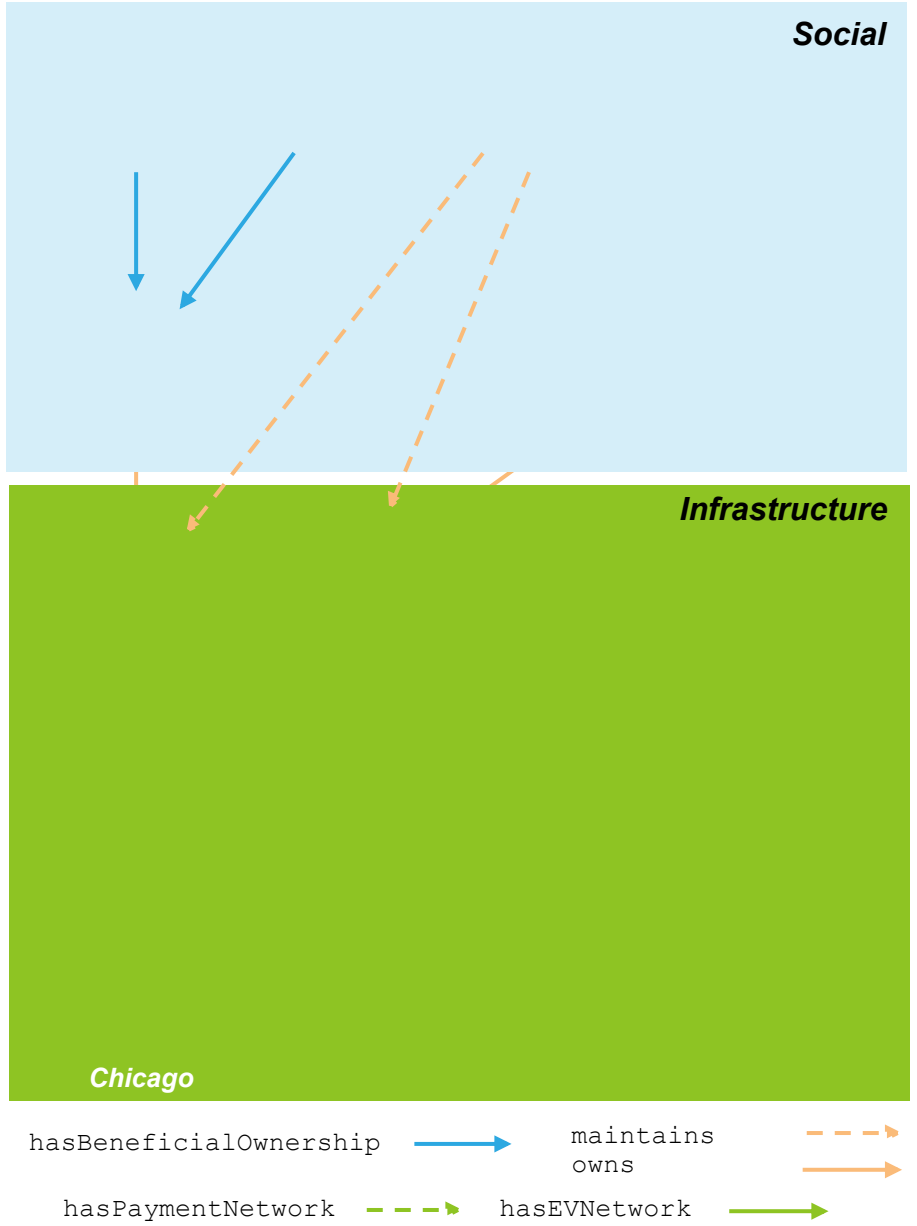
Relations may be expressed as edges.



Analyses Enabled

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

- Semantic Layer ($L_{semantic}$)
  - Inference Algorithms
- Geospatial Layer ($L_{geospatial}$)
  - Spatially-Localized Attacks (SLA) [Ouyang 2016]
- Temporal Layer ($L_{temporal}$)
  - Temporal Motifs [Paranjape et al. 2017]



STNA Network Generation

Architecture and Design

Architecture

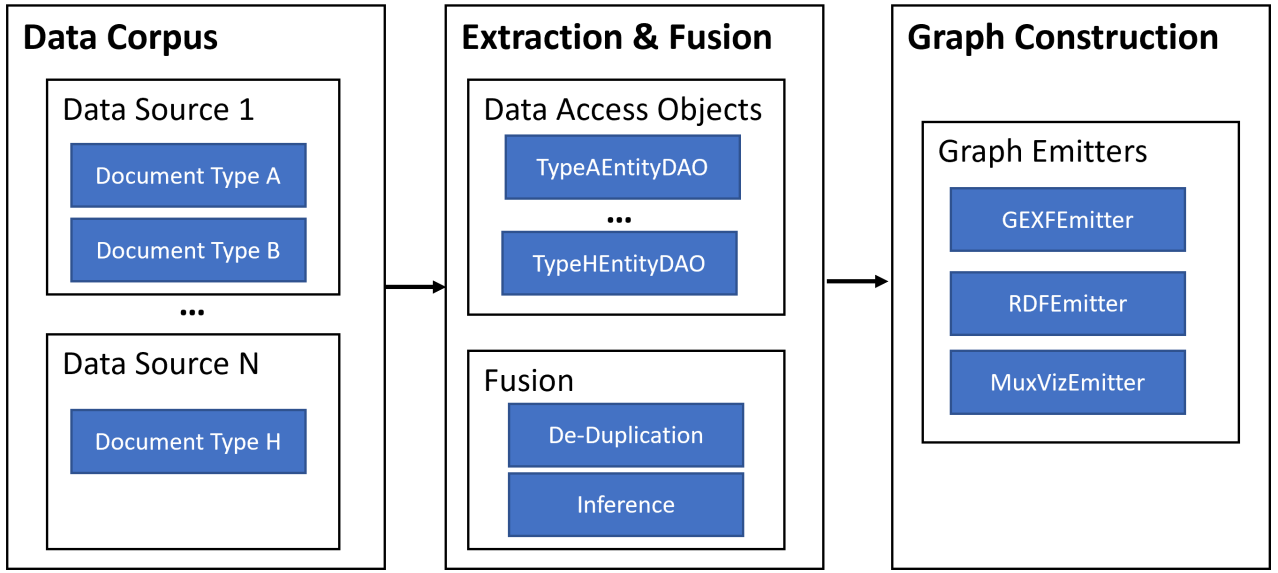
The intent is to construct multilayered networks for adversarial STNA that can be adapted to a wide variety of analyses.

Constructing such networks is difficult

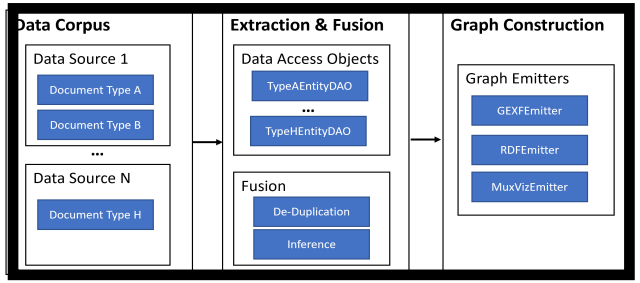
- Diverse, heterogeneous data sources
- Difficult to update, adapt, repurpose

Therefore, we created a data processing pipeline to construct STNA

- Domain model for data access
- Networks composed of explicit data types for vertices, nodes, and other components.

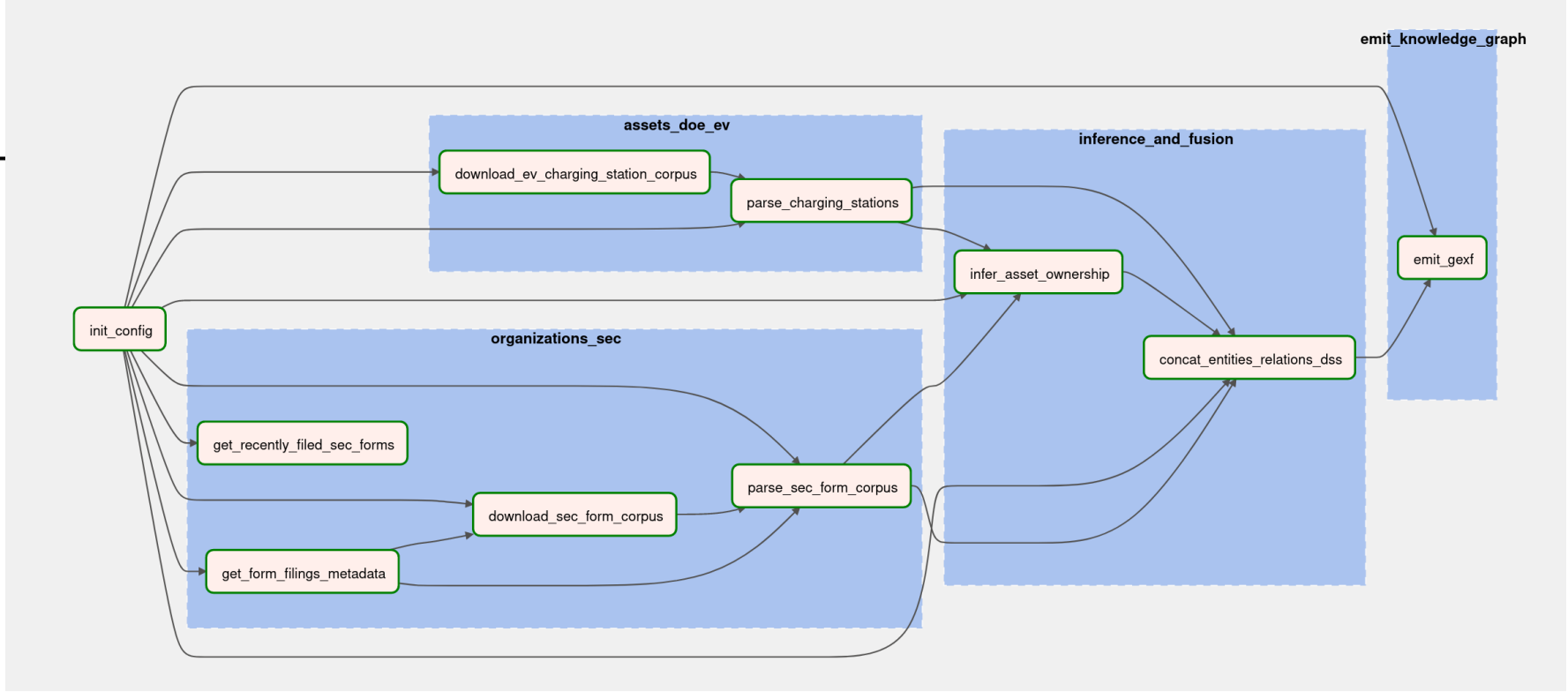


Architecture - Implementation

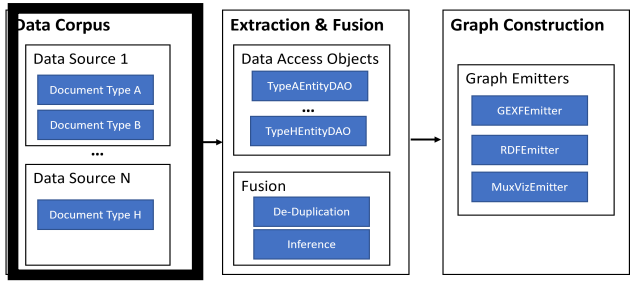


Init Config

```
{'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'}
```



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

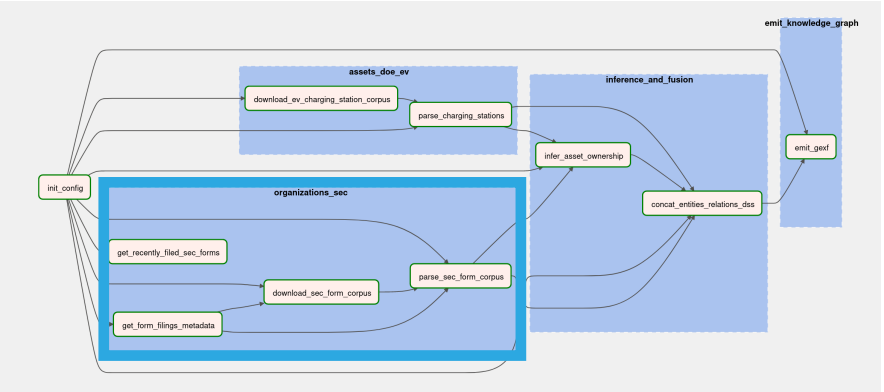
- Twitter [Debreceny 2017]
- Pitchbook
- Facebook
- SEC Data [Bichler et al. 2015]

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

Data Corpus - Implementation



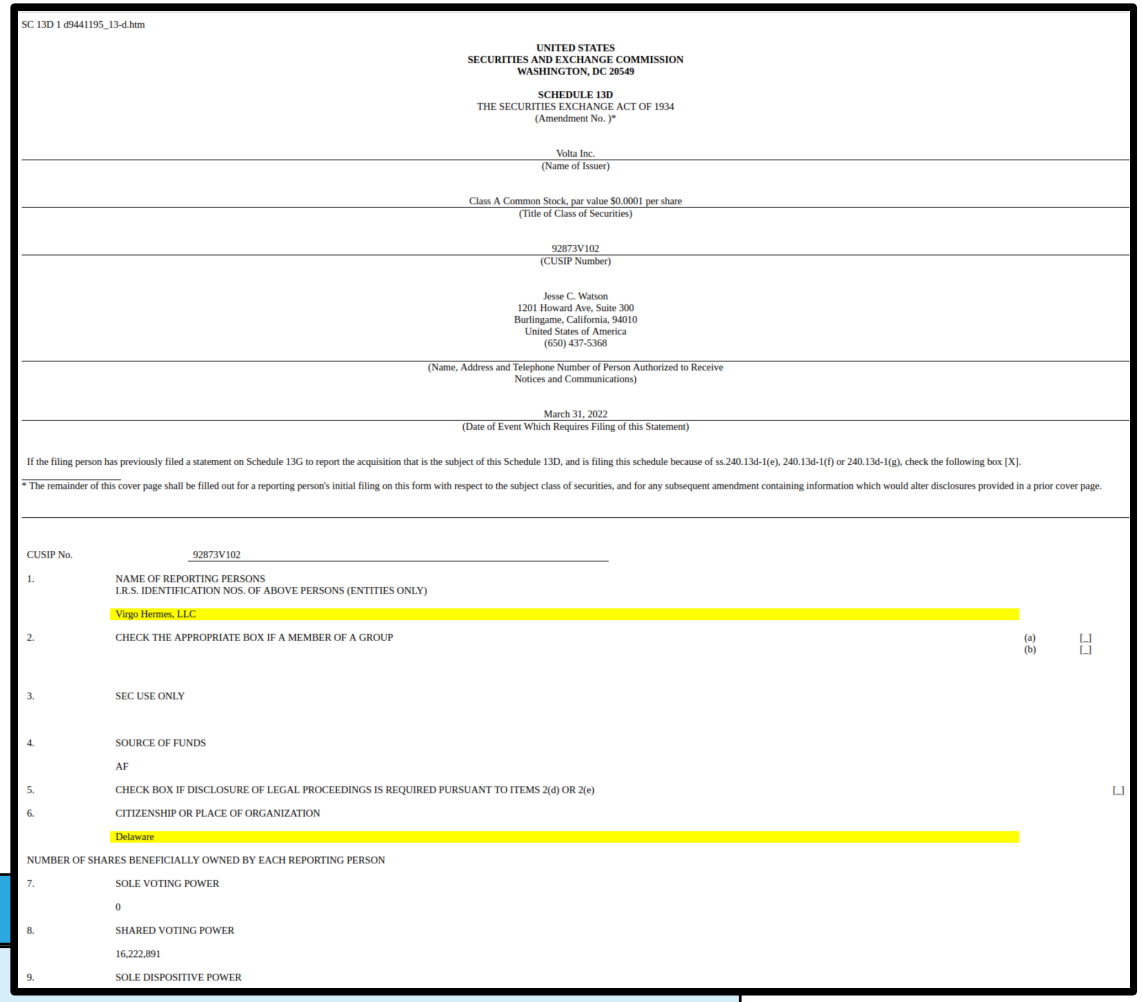
view_filings_metadata

```
(stenv) pasithea@pasithea:~/Documents/LDRD/stna$ python src/bin/view_filings_metadata.py --forms_metadata_path=data/chicago_data/1_23_2023/editorial/form_filings_met
adata.json
Form SC 13D
CIK 0001819584
|     | accessionNumber      | filingDate                 | fileNumber   | primaryDocument              | form    |
|----:|:---------------------|:---------------------------|:-------------|:-----------------------------|:--------|
|  92 | 0000919574-22-002704 | 1970-01-01 00:27:29.721600 | 005-91687    | d9441195_13-d.htm            | SC 13D  |
| 149 | 0001213900-21-053569 | 1970-01-01 00:27:14.688000 | 005-91687    | ea149046-13dtough_volta.htm  | SC 13D  |
| 158 | 0001068238-21-000191 | 1970-01-01 00:27:11.750400 | 005-91687    | volta_scottmercer-sch13d.htm | SC 13D  |
| 159 | 0001068238-21-000190 | 1970-01-01 00:27:11.750400 | 005-91687    | volta_chriswendel-sch13d.htm | SC 13D  |


Form S-4
CIK 0001819584
|     | accessionNumber      | filingDate                 | fileNumber   | primaryDocument          | form    |
|----:|:---------------------|:---------------------------|:-------------|:-------------------------|:--------|
| 229 | 0001213900-21-026615 | 1970-01-01 00:27:01.209600 | 333-256173   | fs42021_tortoiseacq2.htm | S-4     |
```

Social Network Entity Extraction

Social Network – Volta Inc		
SC 13D Filings		
Accession Number	***File Number***	***File Name***
0000919574-22-002704	005-91687	d9441195_13-d.htm
0001213900-21-053569	005-91687	ea149046-13dtough_volta.htm
0001068238-21-000191	005-91687	volta_scottmercer-sch13d.htm
S-4 Filings		
0001213900-21-026615	333-256173	fs42021_tortoiseacq2.htm



SC 13D 1 d9441195_13-d.htm

UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
WASHINGTON, DC 20549

SCHEDULE 13D
THE SECURITIES EXCHANGE ACT OF 1934
(Amendment No.)*

Volta Inc.
(Name of Issuer)

Class A Common Stock, par value $0.0001 per share
(Title of Class of Securities)

92873V102
(CUSIP Number)

Jesse C. Watson
1201 Howard Ave, Suite 300
Burlingame, California, 94010
United States of America
(650) 437-5368

(Name, Address and Telephone Number of Person Authorized to Receive Notices and Communications)

March 31, 2022
(Date of Event Which Requires Filing of this Statement)

If the filing person has previously filed a statement on Schedule 13G to report the acquisition that is the subject of this Schedule 13D, and is filing this schedule because of ss.240.13d-1(e), 240.13d-1(f) or 240.13d-1(g), check the following box [X].

* The remainder of this cover page shall be filled out for a reporting person's initial filing on this form with respect to the subject class of securities, and for any subsequent amendment containing information which would alter disclosures provided in a prior cover page.

CUSIP No. 92873V102

1. NAME OF REPORTING PERSONS
I.R.S. IDENTIFICATION NOS. OF ABOVE PERSONS (ENTITIES ONLY)
Virgo Hermes, LLC

2. CHECK THE APPROPRIATE BOX IF A MEMBER OF A GROUP (a) [_] (b) [_]

3. SEC USE ONLY

4. SOURCE OF FUNDS
AF

5. CHECK BOX IF DISCLOSURE OF LEGAL PROCEEDINGS IS REQUIRED PURSUANT TO ITEMS 2(d) OR 2(e) [_]

6. CITIZENSHIP OR PLACE OF ORGANIZATION
Delaware

NUMBER OF SHARES BENEFICIALLY OWNED BY EACH REPORTING PERSON

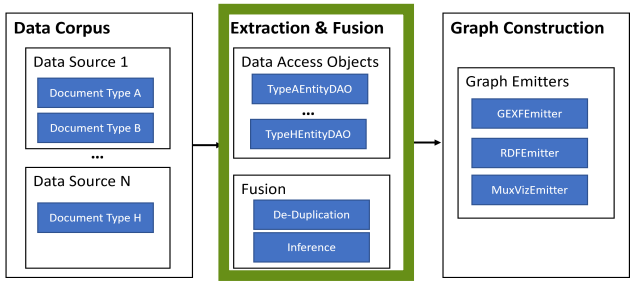
7. SOLE VOTING POWER
0

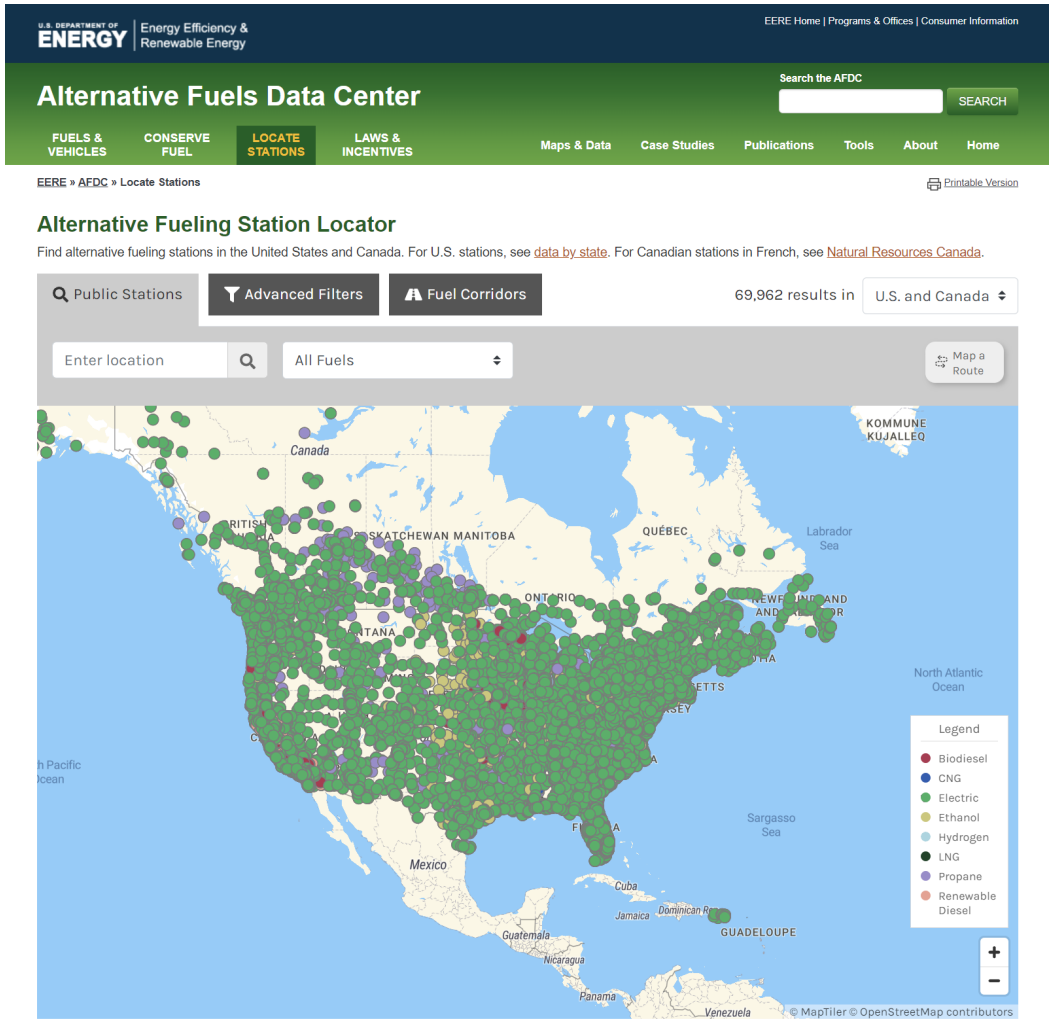
8. SHARED VOTING POWER
16,222,891

9. SOLE DISPOSITIVE POWER

Social Network				
stna_core.Organization				
hasName	***hasLocation***	***ownsPercentage***	***Start date***	***Data source***
Virgo Hermes, LLC	Delaware	10.1%	2022-04-12	d9441195_13-d.htm
Virgo Investment Group LLC	Delaware	10.1%	2022-04-12	d9441195_13-d.htm
Energize Ventures Fund LP	Delaware	6.0%	2021-10-20	Ea149046-13dtough_volta.htm

Critical Infrastructure Sector Entity Extraction



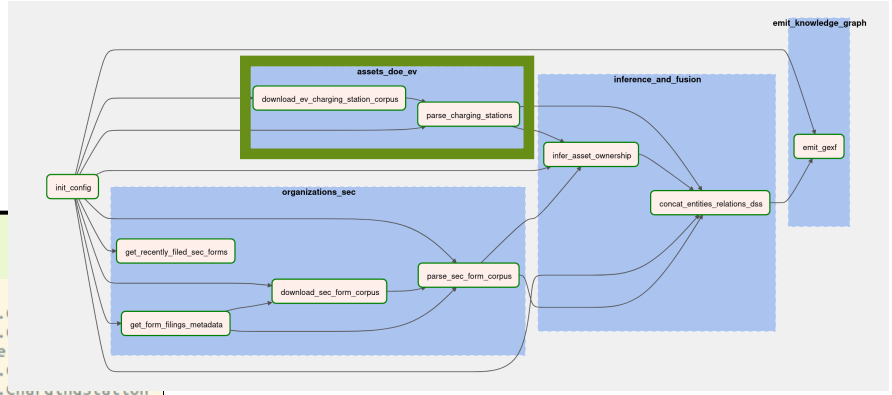


EV Network

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

Entity Extraction - Implementation

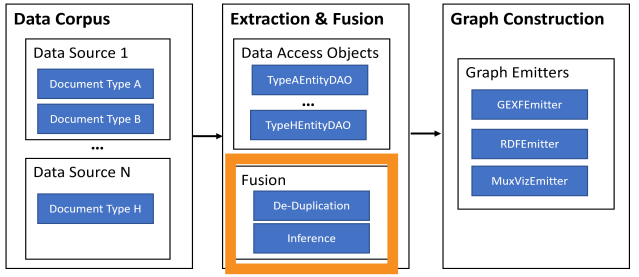


view_entities_relations

	id	access_code	access_days_time	...	start_date	source	
0	196870	private	24 hours daily; Drivers must bring their own J...	...	2021-09-21 00:00:00	https://afdc.energy.gov/stations/	org-influence.
1	Non-Networked	None	None	...	2022-02-10 21:00:18	https://afdc.energy.gov/stations/	org-influence.
2		None	None	...	2022-02-10 21:00:18	https://afdc.energy.gov/stations/	org-influence
3	184701	private	Drivers must bring their own J1772 cordset for...	...	2021-01-15 00:00:00	https://afdc.energy.gov/stations/	org-influence.
4	202792	public	24 hours daily	...	2021-12-18 00:00:00	https://afdc.energy.gov/stations/	org-influence.
5	ChargePoint Network	None	None	...	2023-03-06 23:32:42	https://afdc.energy.gov/stations/	org-influence.ChargingNetwork
6	202791	public	24 hours daily	...	2021-12-18 00:00:00	https://afdc.energy.gov/stations/	org-influence.ChargingStation
7	253419	public	Mon 5:00am - 5:00pm; Tue 5:00am - 5:00pm; Wed ...	...	2023-02-07 00:00:00	https://afdc.energy.gov/stations/	org-influence.ChargingStation
8	215053	public	24 hours daily	...	2022-04-28 00:00:00	https://afdc.energy.gov/stations/	org-influence.ChargingStation
9	215054	public	24 hours daily	...	2022-04-28 00:00:00	https://afdc.energy.gov/stations/	org-influence.ChargingStation
10	238377	public	24 hours daily	...	2022-11-28 00:00:00	https://afdc.energy.gov/stations/	org-influence.ChargingStation
11	FLASH	None	None	...	2023-02-14 15:54:11	https://afdc.energy.gov/stations/	org-influence.ChargingNetwork
12	CREDIT	None	None	...	2023-02-14 15:54:11	https://afdc.energy.gov/stations/	org-influence.PaymentNetwork
13	202794	public	24 hours daily	...	2021-12-18 00:00:00	https://afdc.energy.gov/stations/	org-influence.ChargingStation
14	202793	public	24 hours daily	...	2021-12-18 00:00:00	https://afdc.energy.gov/stations/	org-influence.ChargingStation
15	224650	public	24 hours daily	...	2022-07-30 00:00:00	https://afdc.energy.gov/stations/	org-influence.ChargingStation
16	224651	public	24 hours daily	...	2022-07-30 00:00:00	https://afdc.energy.gov/stations/	org-influence.ChargingStation
17	151749	public	Mon 6:00am - 11:59pm; Tue 6:00am - 11:59pm; We...	...	2015-10-30 00:00:00	https://afdc.energy.gov/stations/	org-influence.ChargingStation
18	Volta	None	None	...	2023-03-06 00:13:18	https://afdc.energy.gov/stations/	org-influence.ChargingNetwork
19	114157	public		...	2016-02-11 00:00:00	https://afdc.energy.gov/stations/	org-influence.ChargingStation
20	Tesla Destination	None	None	...	2023-01-18 15:15:20	https://afdc.energy.gov/stations/	org-influence.ChargingNetwork
21	169013	public		...	2018-06-14 00:00:00	https://afdc.energy.gov/stations/	org-influence.ChargingStation
22	61218	public	24 hours daily	...	2014-04-12 00:00:00	https://afdc.energy.gov/stations/	org-influence.ChargingStation
23	172397	public	24 hours daily	...	2021-01-27 00:00:00	https://afdc.energy.gov/stations/	org-influence.ChargingStation
24	72432	public	24 hours daily	...	2016-01-09 00:00:00	https://afdc.energy.gov/stations/	org-influence.ChargingStation
25	171742	public	24 hours daily	...	2021-01-27 00:00:00	https://afdc.energy.gov/stations/	org-influence.ChargingStation
26	171743	public	24 hours daily	...	2021-01-27 00:00:00	https://afdc.energy.gov/stations/	org-influence.ChargingStation
27	171740	public	24 hours daily	...	2021-01-27 00:00:00	https://afdc.energy.gov/stations/	org-influence.ChargingStation
28	171741	public	24 hours daily	...	2021-01-27 00:00:00	https://afdc.energy.gov/stations/	org-influence.ChargingStation
29	114156	public		...	2016-02-11 00:00:00	https://afdc.energy.gov/stations/	org-influence.ChargingStation
30	202789	public	24 hours daily	...	2021-12-18 00:00:00	https://afdc.energy.gov/stations/	org-influence.ChargingStation
31	202952	public	24 hours daily	...	2021-12-23 00:00:00	https://afdc.energy.gov/stations/	org-influence.ChargingStation
32	80236	public	24 hours daily	...	2016-12-17 00:00:00	https://afdc.energy.gov/stations/	org-influence.ChargingStation
33	236214	public	24 hours daily	...	2022-11-17 00:00:00	https://afdc.energy.gov/stations/	org-influence.ChargingStation
34	235113	public	24 hours daily	...	2022-10-26 00:00:00	https://afdc.energy.gov/stations/	org-influence.ChargingStation
35	238378	public	24 hours daily	...	2022-11-15 00:00:00	https://afdc.energy.gov/stations/	org-influence.ChargingStation
36	224654	public	24 hours daily	...	2022-07-30 00:00:00	https://afdc.energy.gov/stations/	org-influence.ChargingStation
37	224653	public	24 hours daily	...	2022-07-30 00:00:00	https://afdc.energy.gov/stations/	org-influence.ChargingStation
38	164758	public		...	2020-08-01 00:00:00	https://afdc.energy.gov/stations/	org-influence.ChargingStation
39	Blink Network	None	None	...	2023-03-06 22:58:24	https://afdc.energy.gov/stations/	org-influence.ChargingNetwork
40	164418	public	24 hours daily	...	2020-07-22 00:00:00	https://afdc.energy.gov/stations/	org-influence.ChargingStation
41	205057	public	24 hours daily	...	2022-01-20 00:00:00	https://afdc.energy.gov/stations/	org-influence.ChargingStation
42	202797	public	24 hours daily	...	2021-12-18 00:00:00	https://afdc.energy.gov/stations/	org-influence.ChargingStation
43	192898	public	24 hours daily	...	2021-07-16 00:00:00	https://afdc.energy.gov/stations/	org-influence.ChargingStation
44	151747	public	Mon 6:00am - 11:59pm; Tue 6:00am - 11:59pm; We...	...	2015-11-25 00:00:00	https://afdc.energy.gov/stations/	org-influence.ChargingStation
45	185392	public	24 hours daily	...	2021-02-26 00:00:00	https://afdc.energy.gov/stations/	org-influence.ChargingStation
46	114161	public		...	2019-01-02 00:00:00	https://afdc.energy.gov/stations/	org-influence.ChargingStation
47	202908	public	24 hours daily	...	2021-12-22 00:00:00	https://afdc.energy.gov/stations/	org-influence.ChargingStation
48	202796	public	24 hours daily	...	2021-12-18 00:00:00	https://afdc.energy.gov/stations/	org-influence.ChargingStation
49	202956	public	24 hours daily	...	2021-12-23 00:00:00	https://afdc.energy.gov/stations/	org-influence.ChargingStation

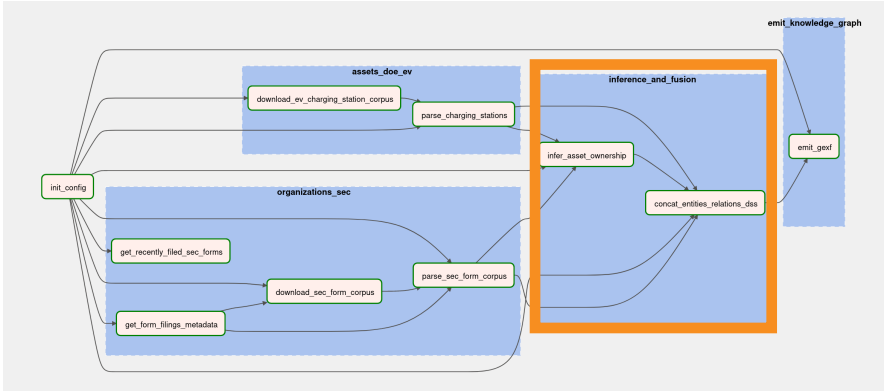
[50 rows x 74 columns]

Fusion



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
alt-fuel-stations.EVChargingNetwork			
ChargePoint Network	None	n/a	n/a
Tesla Destination	None	n/a	n/a
Blink Network	None	n/a	n/a

Fusion - Implementation



view_entities_relations

	subject_id	relation	object_id	subject_name	...	start_date	source	update_date	sort_date
520	A D M V	isNetworkOf	166665	0	...	1970-01-01 00:00:00.000000	https://afdc.energy.gov/stations/	1970-01-01 00:26:55.504937	2021-03-11 23:22:17
519	EV Connect	isNetworkOf	166665	0	...	1970-01-01 00:00:00.000000	https://afdc.energy.gov/stations/	1970-01-01 00:26:55.504937	2021-03-11 23:22:17
314	Non-Networked	isNetworkOf	60987	0	...	1970-01-01 00:00:00.000000	https://afdc.energy.gov/stations/	1970-01-01 00:26:55.504937	2021-03-11 23:22:17
666	Non-Networked	isNetworkOf	184418	0	...	1970-01-01 00:00:00.000000	https://afdc.energy.gov/stations/	1970-01-01 00:27:08.035312	2021-08-04 00:01:52
5	0001879460	acquiresBeneficialInterest	0001819584	Mercer Scott	...	1970-01-01 00:27:11.750400	build/chicago/1_23_2023/SEC/0001819584/0001068...	1970-01-01 00:00:00.000000	2021-09-16
6	0001879459	acquiresBeneficialInterest	0001819584	Wendel Christopher	...	1970-01-01 00:27:11.750400	build/chicago/1_23_2023/SEC/0001819584/0001068...	1970-01-01 00:00:00.000000	2021-09-16
9	Energize Ventures Fund LP	acquiresBeneficialInterest	0001819584	Energize Ventures Fund LP	...	1970-01-01 00:27:14.688000	build/chicago/1_23_2023/SEC/0001819584/0001213...	1970-01-01 00:00:00.000000	2021-10-20
7	0001879633	acquiresBeneficialInterest	0001819584	Tough John J.	...	1970-01-01 00:27:14.688000	build/chicago/1_23_2023/SEC/0001819584/0001213...	1970-01-01 00:00:00.000000	2021-10-20
8	John Tough	acquiresBeneficialInterest	0001819584	John Tough	...	1970-01-01 00:27:14.688000	build/chicago/1_23_2023/SEC/0001819584/0001213...	1970-01-01 00:00:00.000000	2021-10-20
10	Energize Growth Fund I LP	acquiresBeneficialInterest	0001819584	Energize Growth Fund I LP	...	1970-01-01 00:27:14.688000	build/chicago/1_23_2023/SEC/0001819584/0001213...	1970-01-01 00:00:00.000000	2021-10-20
11	Energize Growth I GP LLC	acquiresBeneficialInterest	0001819584	Energize Growth I GP LLC	...	1970-01-01 00:27:14.688000	build/chicago/1_23_2023/SEC/0001819584/0001213...	1970-01-01 00:00:00.000000	2021-10-20
12	EV Volta SPV LLC	acquiresBeneficialInterest	0001819584	EV Volta SPV LLC	...	1970-01-01 00:27:14.688000	build/chicago/1_23_2023/SEC/0001819584/0001213...	1970-01-01 00:00:00.000000	2021-10-20
13	Energize Ventures GP LLC	acquiresBeneficialInterest	0001819584	Energize Ventures GP LLC	...	1970-01-01 00:27:14.688000	build/chicago/1_23_2023/SEC/0001819584/0001213...	1970-01-01 00:00:00.000000	2021-10-20
297	A CREDIT D Debit M V	isNetworkOf	187544	0	...	1970-01-01 00:00:00.000000	https://afdc.energy.gov/stations/	1970-01-01 00:27:24.522149	2022-02-10 19:42:29
443	Non-Networked	isNetworkOf	43358	0	...	1970-01-01 00:00:00.000000	https://afdc.energy.gov/stations/	1970-01-01 00:27:24.522149	2022-02-10 19:42:29
296	Non-Networked	isNetworkOf	187544	0	...	1970-01-01 00:00:00.000000	https://afdc.energy.gov/stations/	1970-01-01 00:27:24.522149	2022-02-10 19:42:29
511	Non-Networked	isNetworkOf	53859	0	...	1970-01-01 00:00:00.000000	https://afdc.energy.gov/stations/	1970-01-01 00:27:24.522149	2022-02-10 19:42:29
232	AMPUP	isNetworkOf	169699	0	...	1970-01-01 00:00:00.000000	https://afdc.energy.gov/stations/	1970-01-01 00:27:24.522149	2022-02-10 19:42:29
15	Non-Networked	isNetworkOf	184701	0	...	1970-01-01 00:00:00.000000	https://afdc.energy.gov/stations/	1970-01-01 00:27:24.526818	2022-02-10 21:00:18
14	Non-Networked	isNetworkOf	196870	0	...	1970-01-01 00:00:00.000000	https://afdc.energy.gov/stations/	1970-01-01 00:27:24.526818	2022-02-10 21:00:18

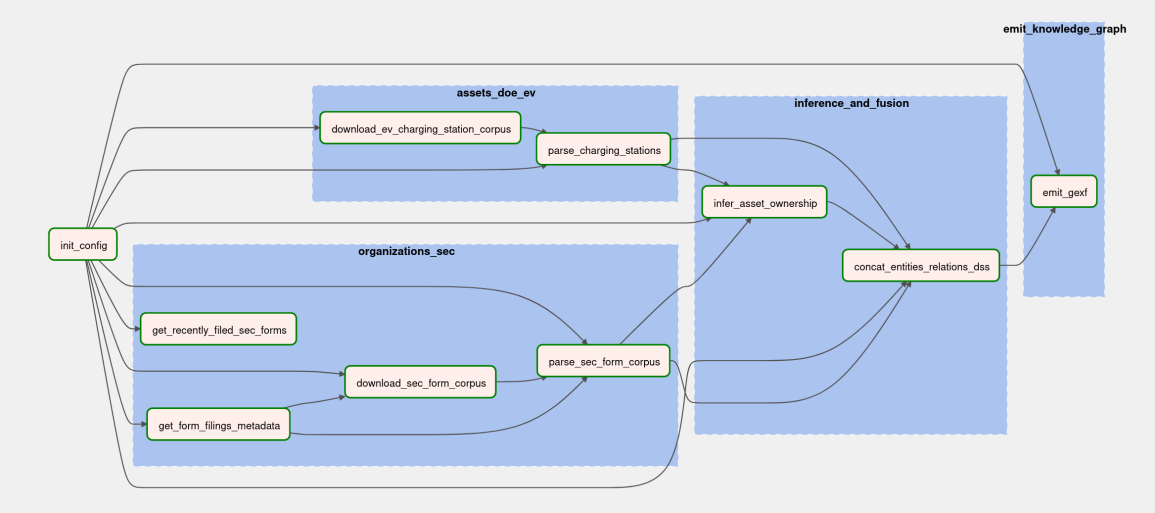
Iterative Discovery

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'}
```

Regional Infrastructure Asset Ownership

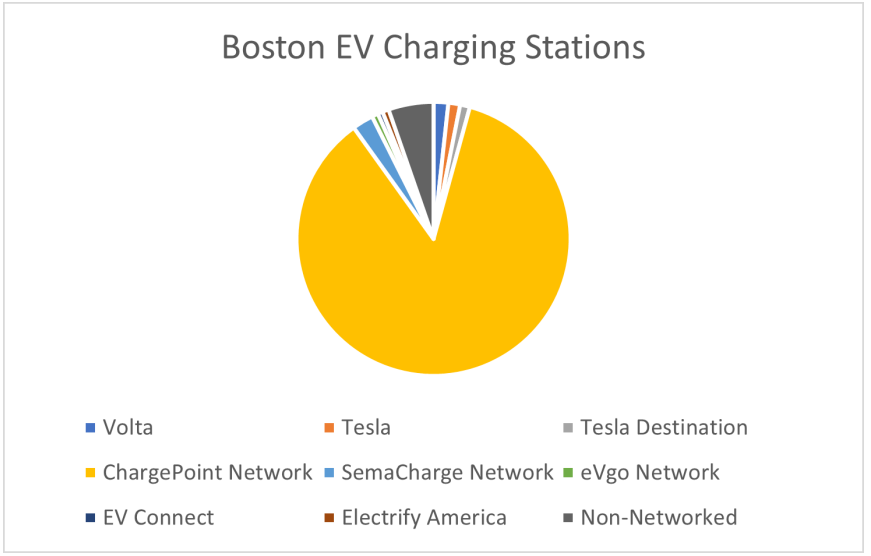
Semantic and Geospatial Analysis

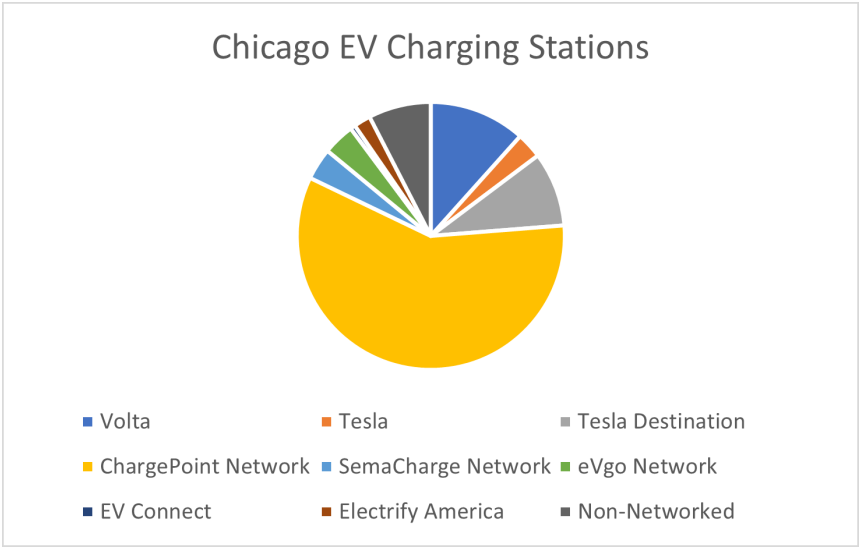
Resource Ownership within a Region

Our intent is for adversarial STNA networks to enable a wide variety of analyses of *organizational influence over physical infrastructure systems*.

Example: Consider the ownership of the communications network upon which EV Charging Stations in a region depend.

- *Semantic attributes* ($L_{semantic}$) enable us to infer an ownership (`owns`) relation given the name of the `EVChargingNetwork` and an `Organization`.
- The data analysis pipeline enables comparison across different regions.

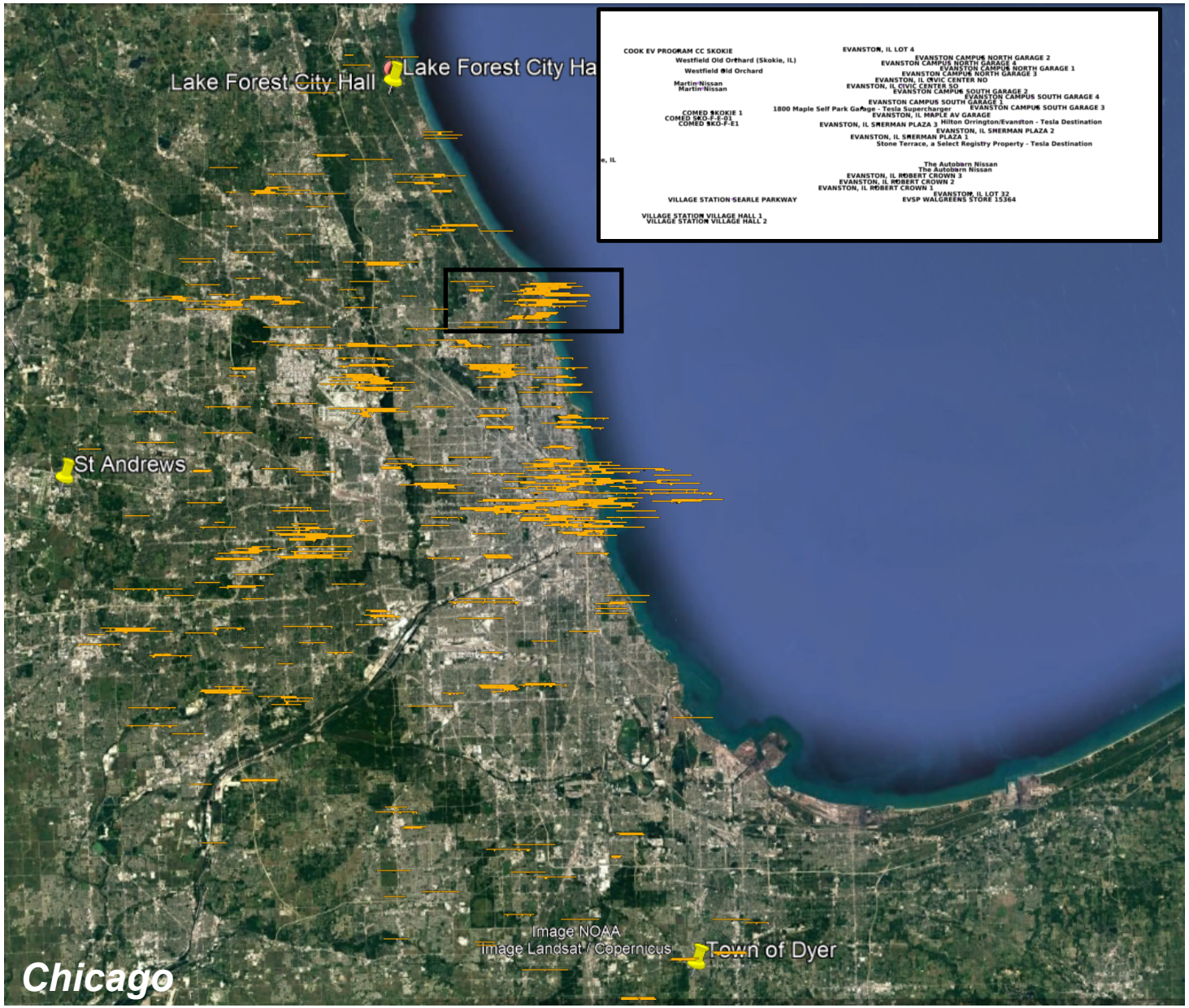




Resource Ownership within a Region

Geospatial Attributes ($L_{geospatial}$) within the Critical Infrastructure layers enable us to consider organizational influence over specific region.

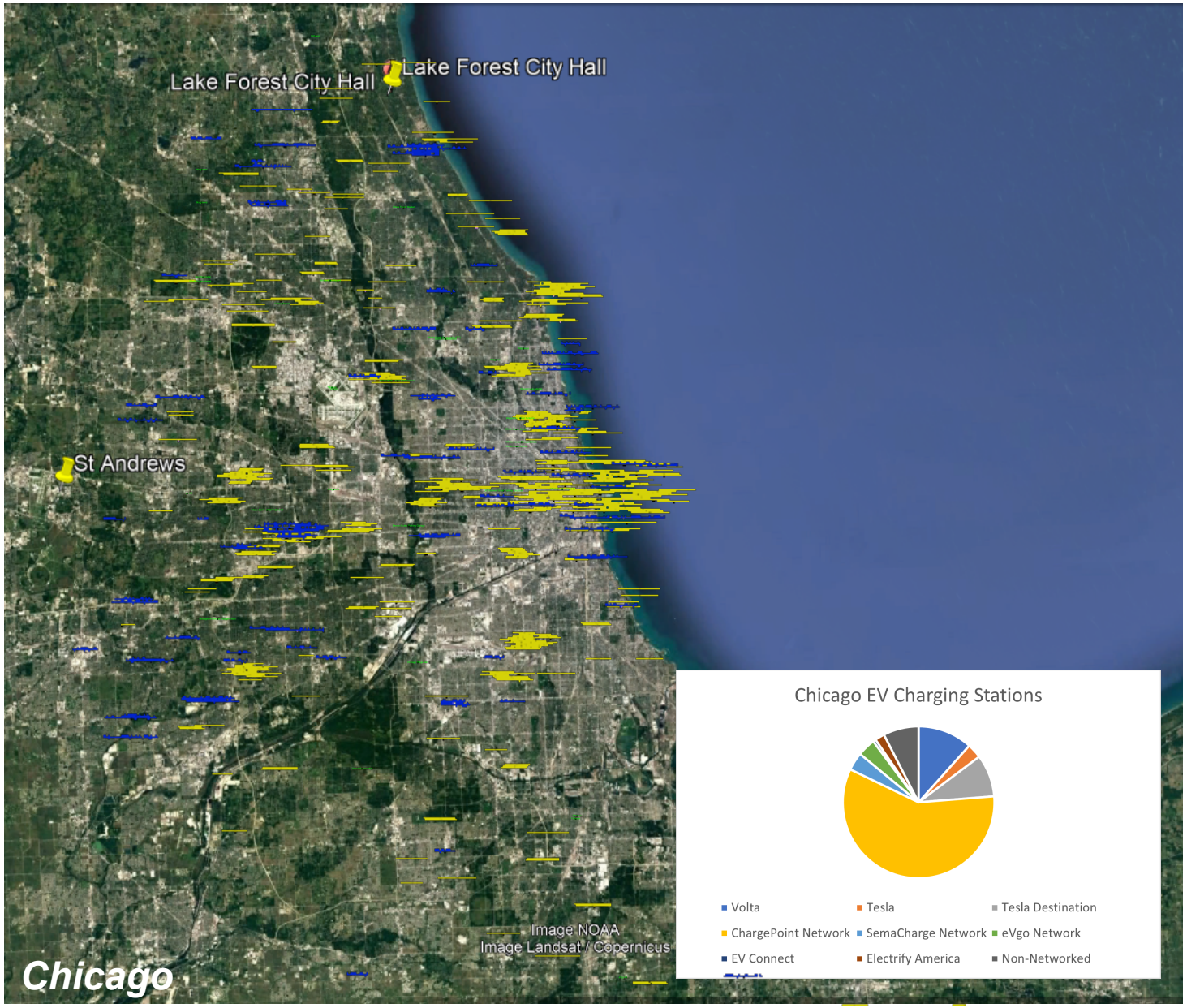
- This provides more detail than a simple pie chart of proportions
- Enables the ability to zoom in on a given region of interest



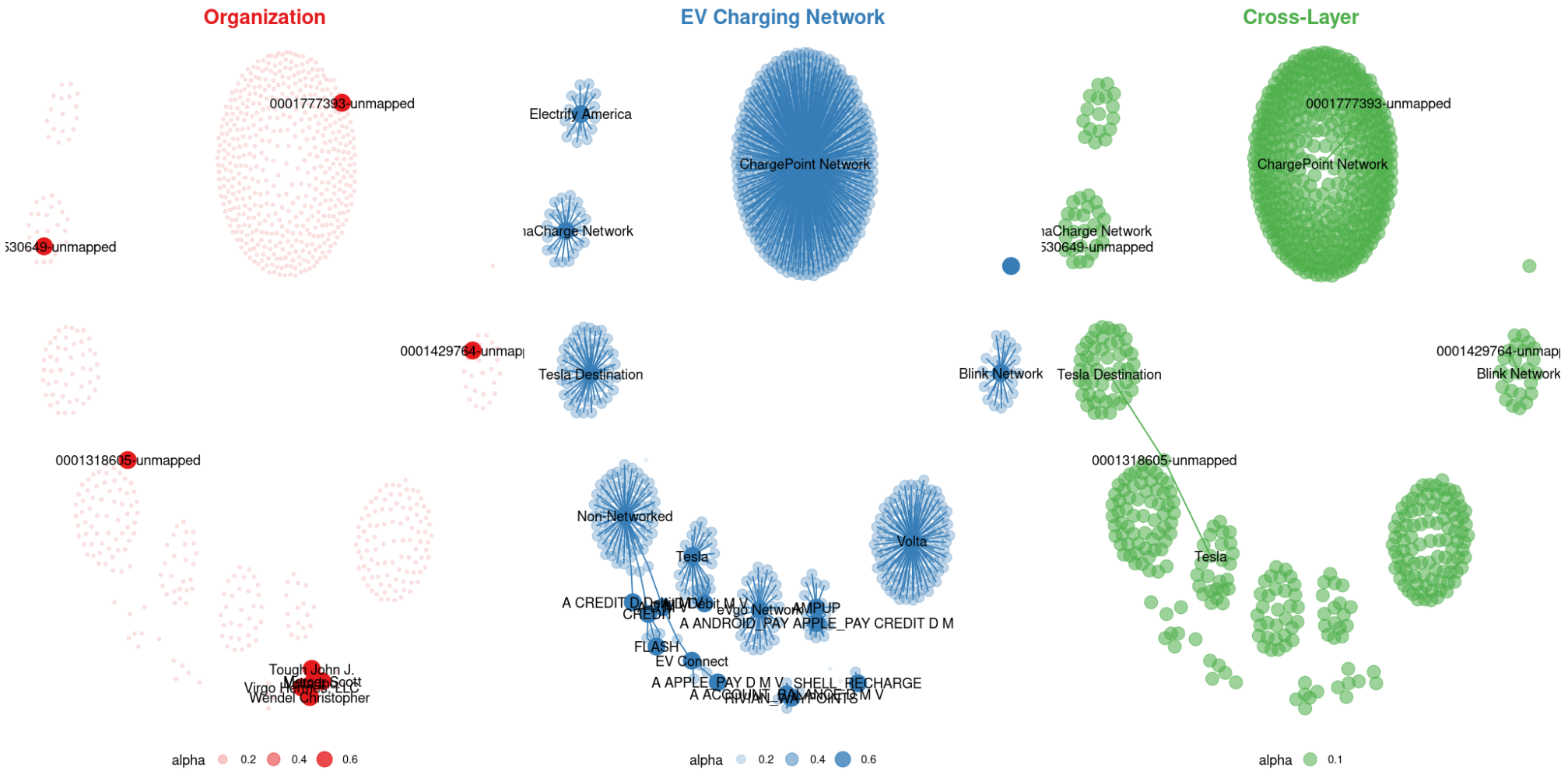
Resource Ownership within a Region

Geospatial Attributes ($L_{geospatial}$) within the Critical Infrastructure layers enable us to consider organizational influence over specific region.

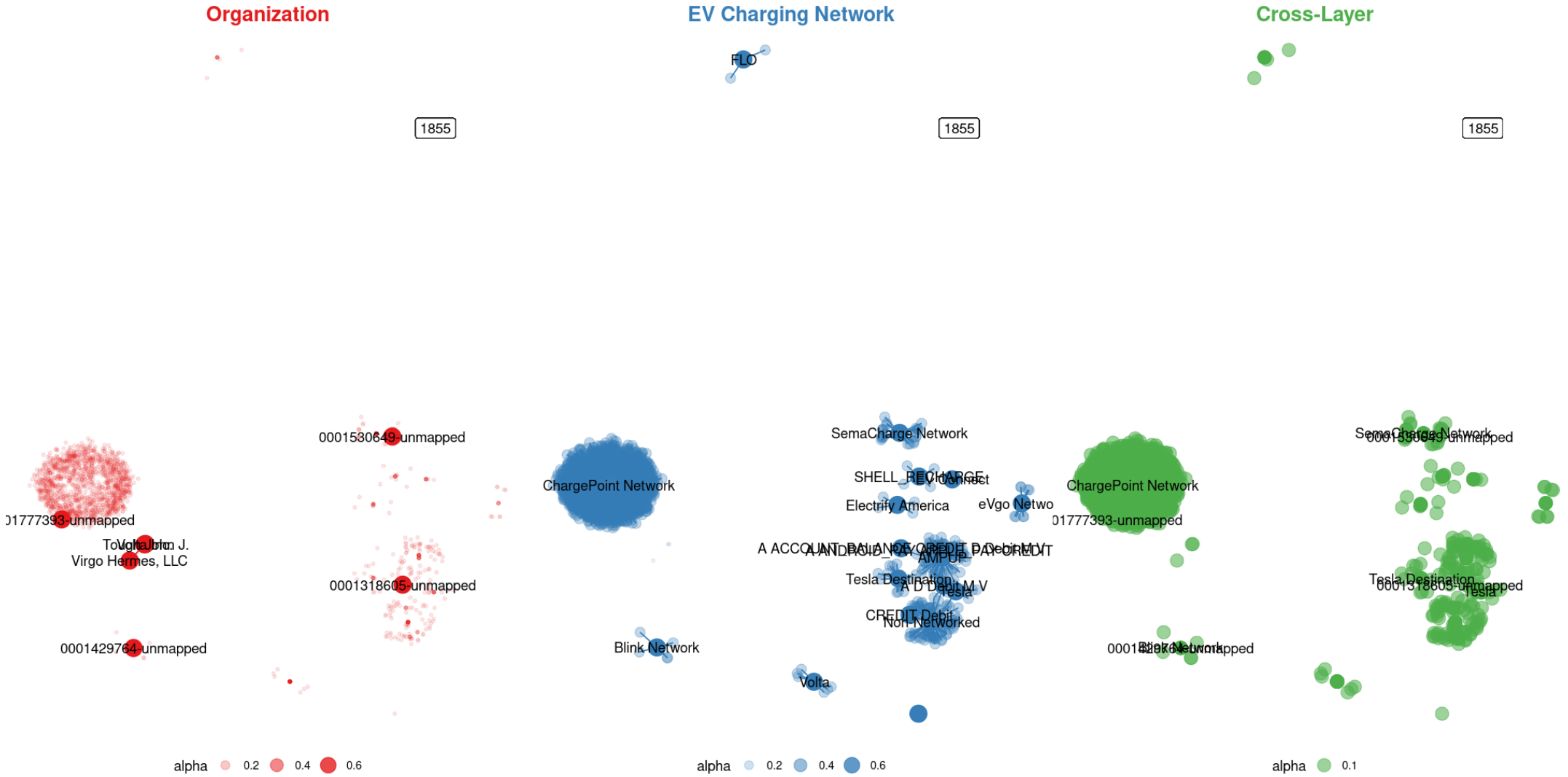
- This provides more detail than a simple pie chart of proportions
- Enables the ability to zoom in on a given region of interest and see who has influence and where
  - ChargePoint
  - Volta
  - eVgo



EV Charging Station Ownership Around Chicago



EV Charging Station Ownership Around Boston



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

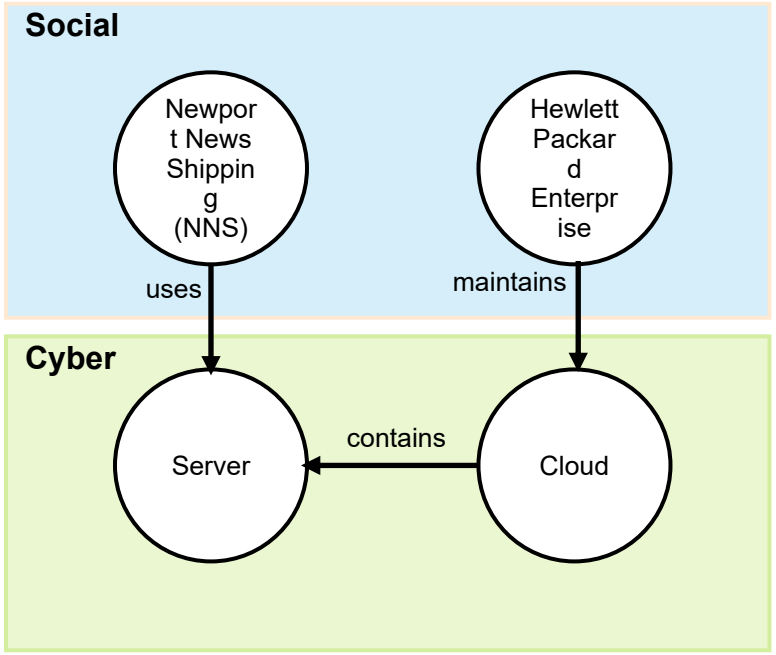
Electric tanks and upgraded targeting drones | Defense News Weekly Full Episode 10.22.22

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:

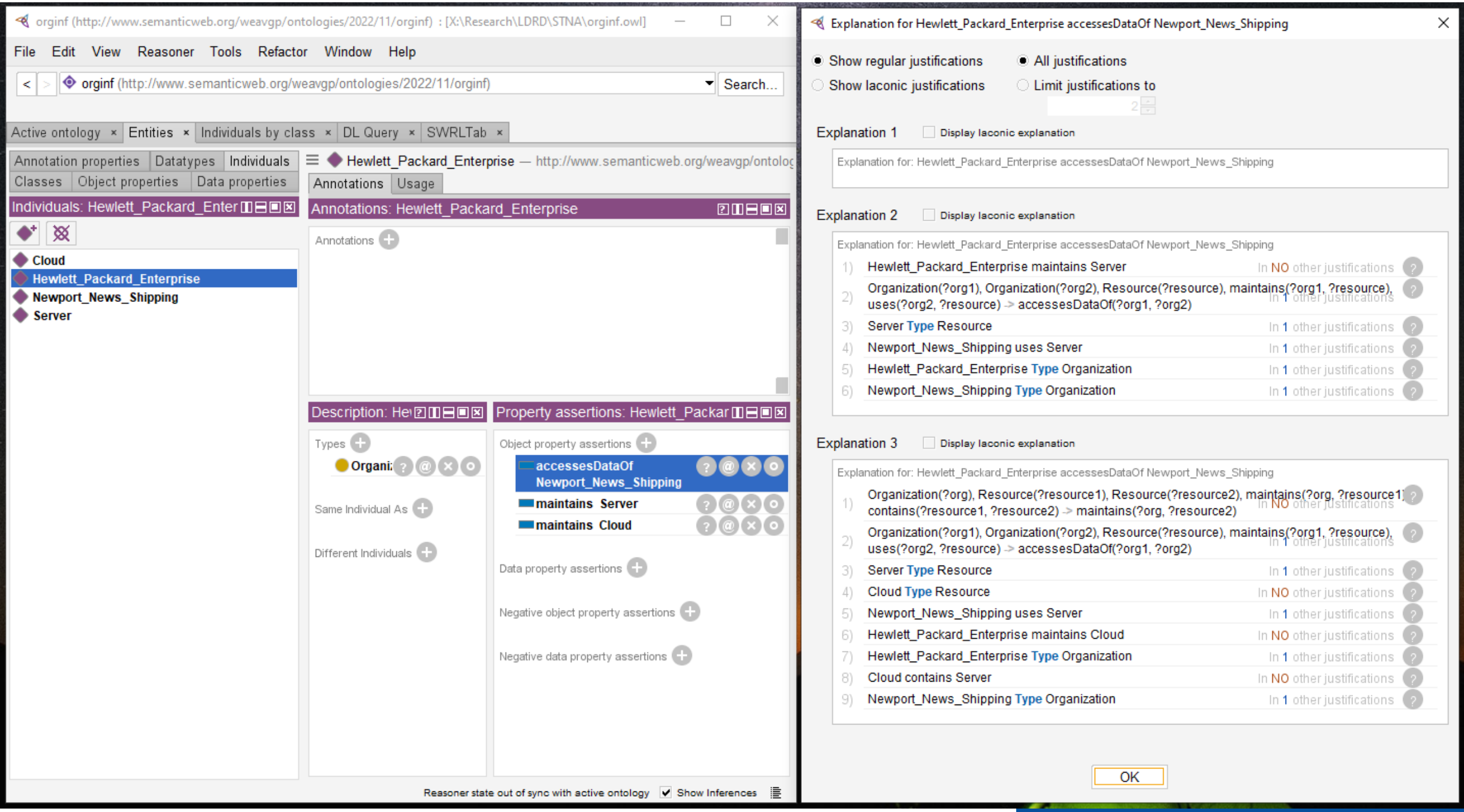
From time t1_1 to time t2_1.

Inference:

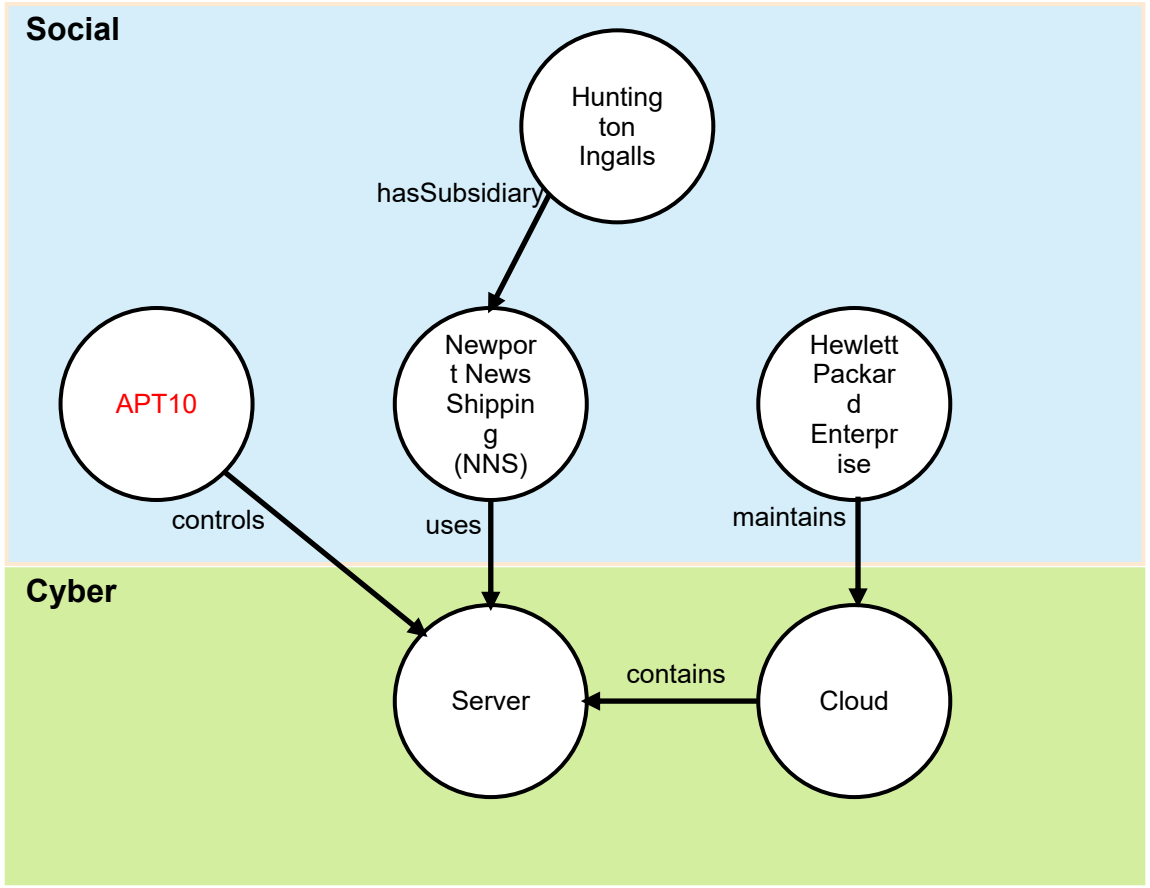
1. <org1> maintains <resource1> & <resource1> contains <resource2> → <org1> maintains <resource2>
2. <org1> maintains <resource2> & <org2> uses <resource2> □ <org1> accessesDataOf <org2>

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:

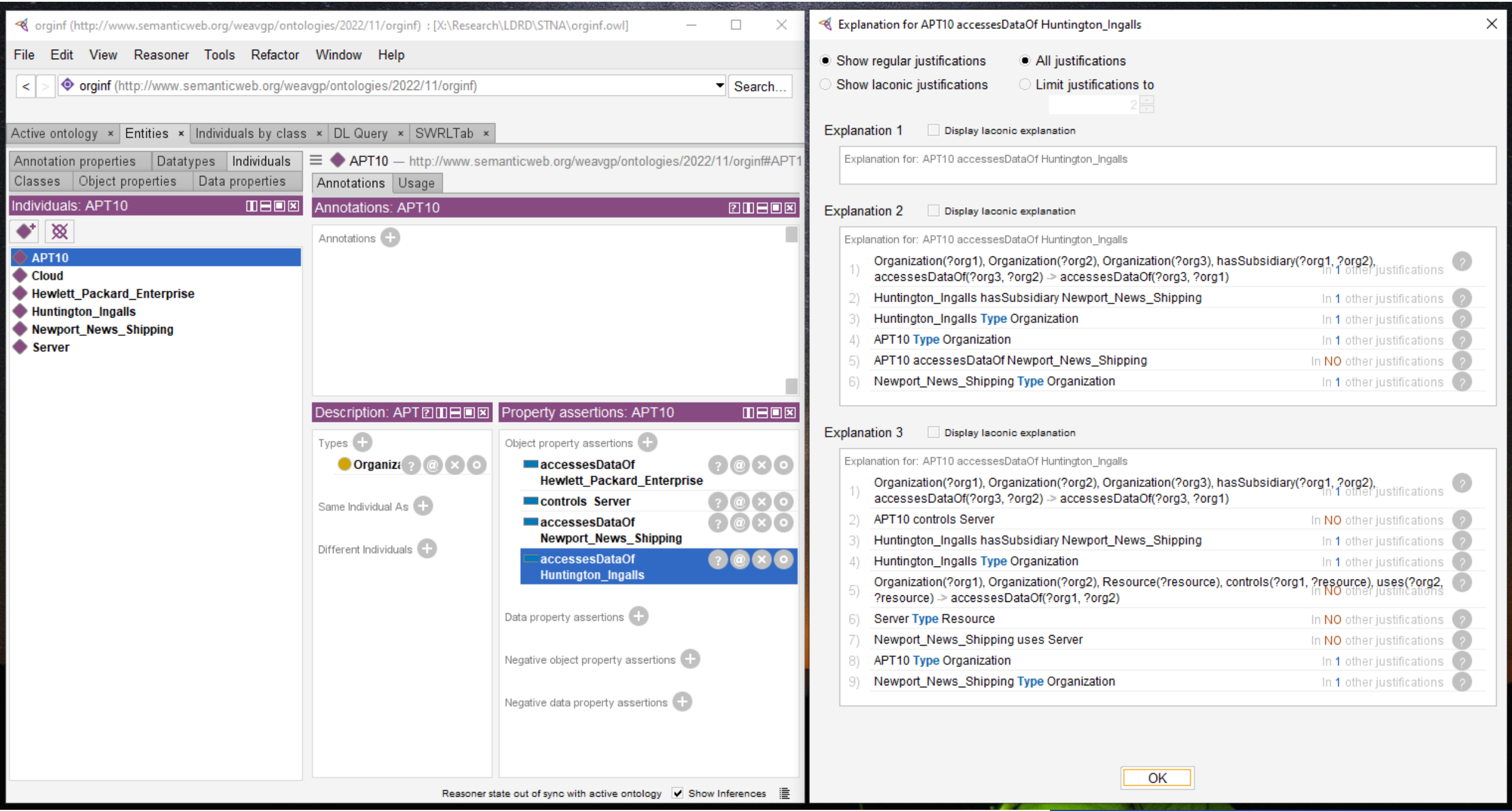
1. <org1> maintains <resource1> & <resource1> contains <resource2> → <org1> maintains <resource2>
2. <org1> maintains <resource2> & <org2> uses <resource2> □ <org1> accessesDataOf <org2>
3. <org1> controls <resource2> & <org2> uses <resource2> □ <org1> accessesDataOf <org2>
4. <org1> controls <resource2>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

Conclusions

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.

Our Approach: 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.
- Support a variety of analyses using semantic, geospatial, and temporal attributes.

Social	Acquisition	Ownership	Company Ownership Proxy	Due Diligence for Mergers & Acquisitions	Foreign-Owned Facilities
	Use	Board Membership	Board Membership Proxy	Legal Subpoena	Disinformation
	Leasing	Asset Maintenance		Digital Twin Creation	Degrade Service Quality
Cyber	Drive-by Compromise	Hardcoded Credentials	Change Operating Mode	Network Connection Enumeration	Unauthorized Command Message

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.