INL/CON-23-71157-Revision-1

Comparison of Socio-Technical Threat Models for Electrical Vehicle Charging Stations

June 2023

Gabriel Arthur Weaver, Daniel A. Eisenberg

DISCLAIMER

This information was prepared as an account of work sponsored by an agency of the U.S. Government. Neither the U.S. Government nor any agency thereof, nor any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness, of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the U.S. Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the U.S. Government or any agency thereof.

INL/CON-23-71157-Revision-1

Comparison of Socio-Technical Threat Models for Electrical Vehicle Charging Stations

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

Comparison of Socio-Technical Threat Models

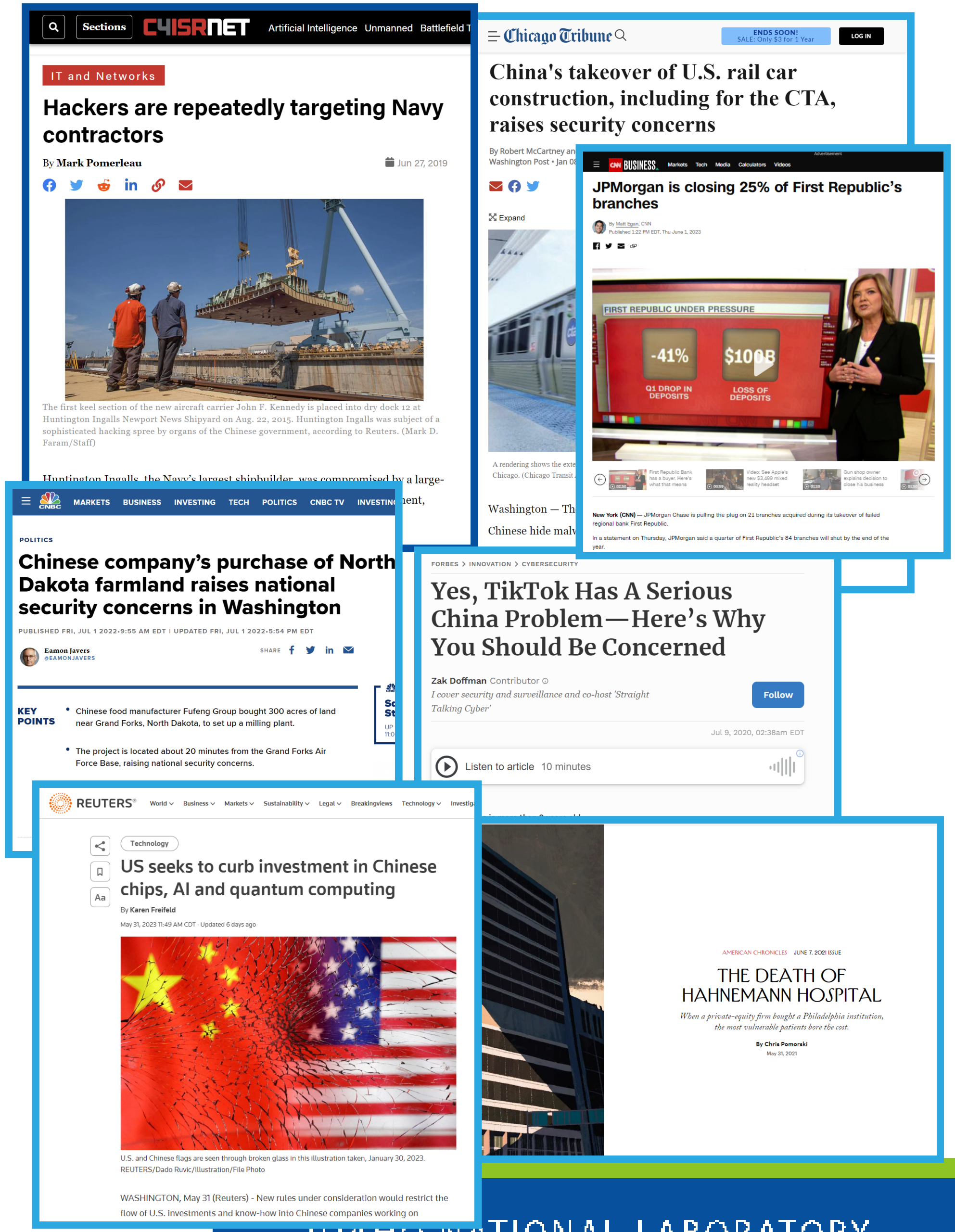
MORS

Motivation

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.

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



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-

ent,

China's takeover of U.S. rail car construction, including for the CTA, raises security concerns

By Robert McCartney an
Washington Post • Jan 0

Expand

A rendering shows the exte
Chicago. (Chicago Transit

Washington — Th

Chinese hide malw

JPMorgan is closing 25% of First Republic’s branches

By Matt Egan, CNN
Published 1:22 PM EDT, Thu June 1, 2023

FIRST REPUBLIC UNDER PRESSURE
-41%
Q1 DROP IN DEPOSITS
$100B
LOSS OF DEPOSITS
First Republic Bank has a buyer. Here's what that means
Video: See Apple's new $3,499 mixed reality headset
Gun shop owner explains decision to close his business

New York (CNN) — JPMorgan Chase is pulling the plug on 21 branches acquired during its takeover of failed regional bank First Republic.

In a statement on Thursday, JPMorgan said a quarter of First Republic’s 84 branches will shut by the end of the year.

POLITICS

Chinese company’s purchase of North Dakota farmland raises national security concerns in Washington

PUBLISHED FRI, JUL 1 2022·9:55 AM EDT | UPDATED FRI, JUL 1 2022·5:54 PM EDT

Eamon Javers
@EAMONJAVERS

SHARE

KEY POINTS

- Chinese food manufacturer Fufeng Group bought 300 acres of land near Grand Forks, North Dakota, to set up a milling plant.
- The project is located about 20 minutes from the Grand Forks Air Force Base, raising national security concerns.

FORBES > INNOVATION > CYBERSECURITY

Yes, TikTok Has A Serious China Problem—Here’s Why You Should Be Concerned

Zak Doffman Contributor
I cover security and surveillance and co-host 'Straight Talking Cyber'

Follow

Jul 9, 2020, 02:38am EDT

Listen to article 10 minutes

REUTERS
World Business Markets Sustainability Legal Breakingviews Technology Investig

Technology

US seeks to curb investment in Chinese chips, AI and quantum computing

By Karen Freifeld
May 31, 2023 11:49 AM CDT · Updated 6 days ago

U.S. and Chinese flags are seen through broken glass in this illustration taken, January 30, 2023. REUTERS/Dado Ruvic/Illustration/File Photo

WASHINGTON, May 31 (Reuters) - New rules under consideration would restrict the flow of U.S. investments and know-how into Chinese companies working on

AMERICAN CHRONICLES JUNE 7, 2021 ISSUE

THE DEATH OF HAHNEMANN HOSPITAL

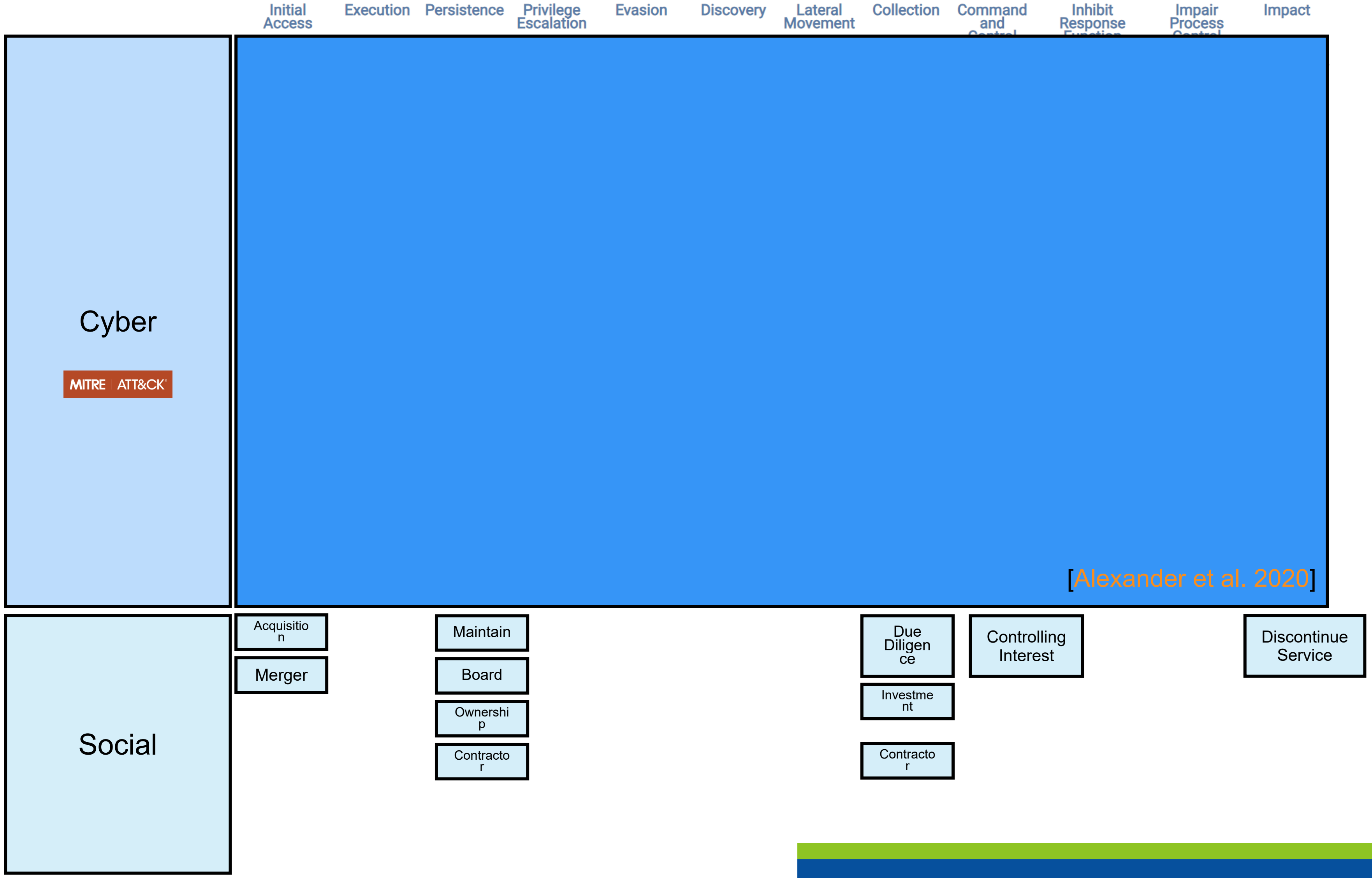
When a private-equity firm bought a Philadelphia institution, the most vulnerable patients bore the cost.

By Chris Pomorski
May 31, 2021

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

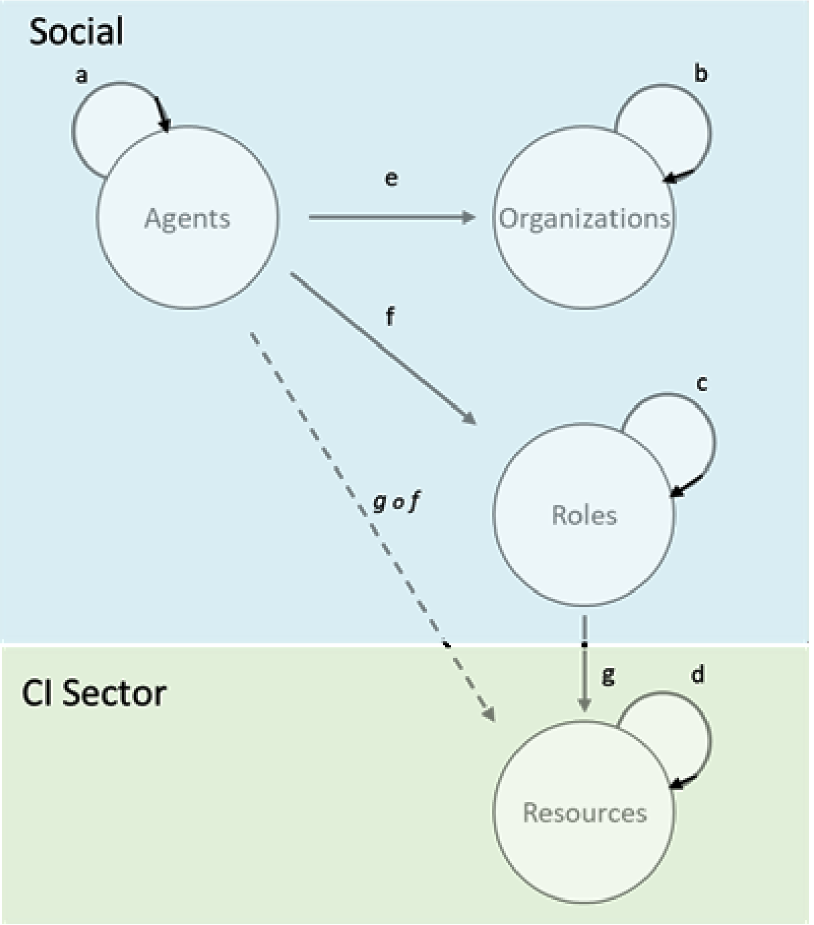
Our research focuses on adversarial techniques in the business domain that affect infrastructure.

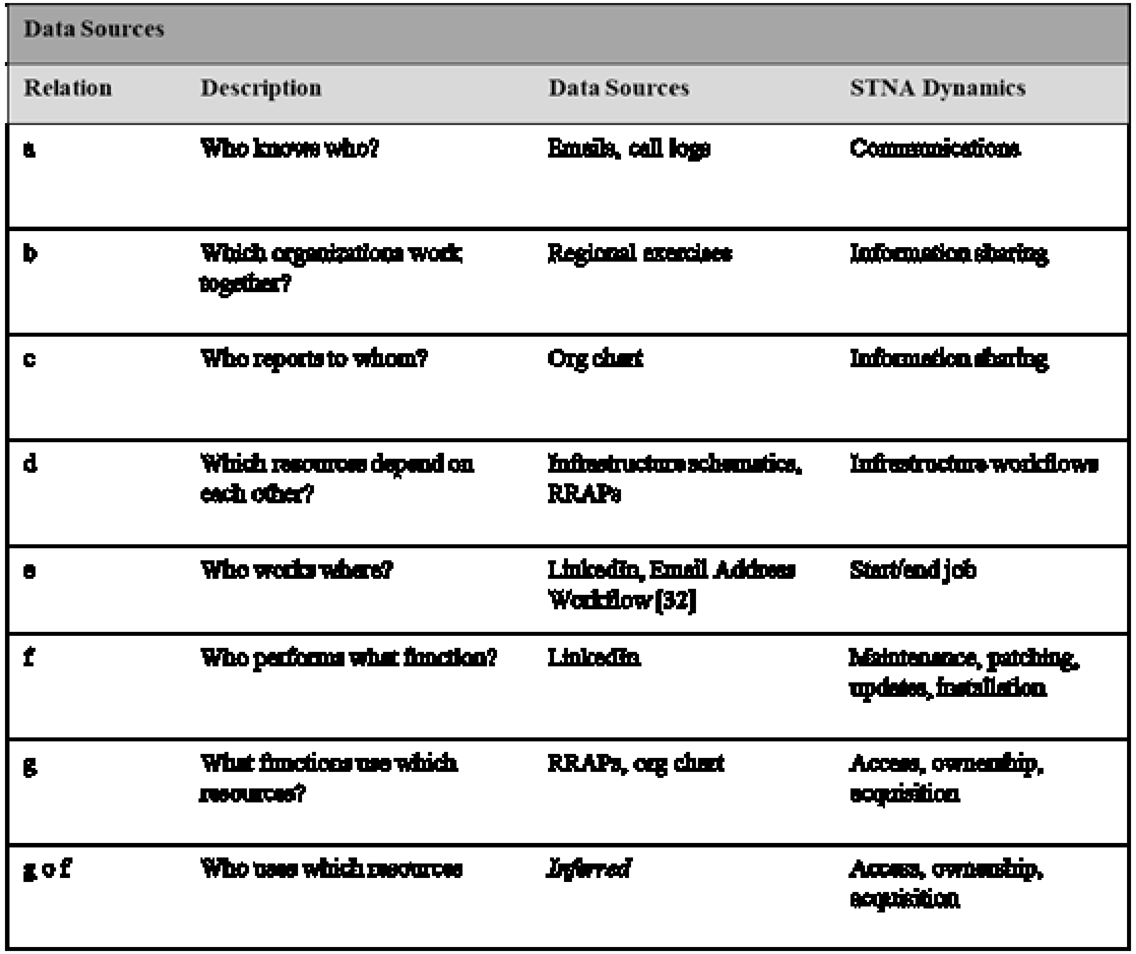
- Want to think about how such techniques across domains can be composed by adversaries.
- Cross-domain ‘kill-chains’ (e.g. [Assante et al. 2015])



	Initial Access	Execution	Persistence	Privilege Escalation	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
Cyber MITRE | ATT&CK												[Alexander et al. 2020]
Social	Acquisition Merger		Maintain Board Ownership Contractor					Due Diligence Investment Contractor	Controlling Interest			Discontinue Service

Socio-Technical Relations Considered





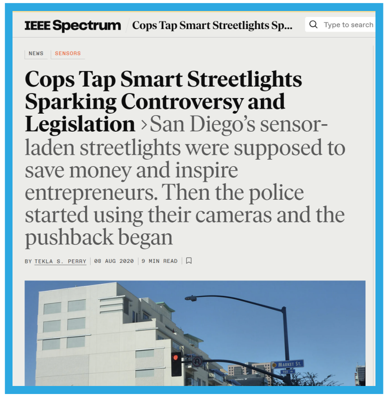
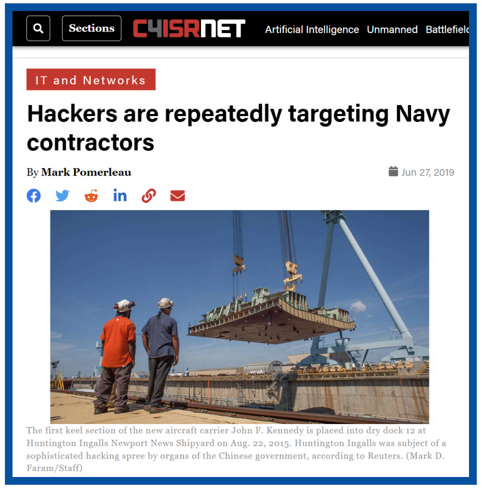
Data Sources			
Relation	Description	Data Sources	STNA Dynamics
a	Who knows who?	Emails, call logs	Communications
b	Which organizations work together?	Regional exercises	Information sharing
c	Who reports to whom?	Org chart	Information sharing
d	Which resources depend on each other?	Infrastructure schematics, 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

Outline

- Introduction
- Socio-Technical Adversarial Tactics
  - Loss of Availability (T0826) for Impact
  - Data Repositories (T0811) for Collection
- Initial Results
- Conclusion

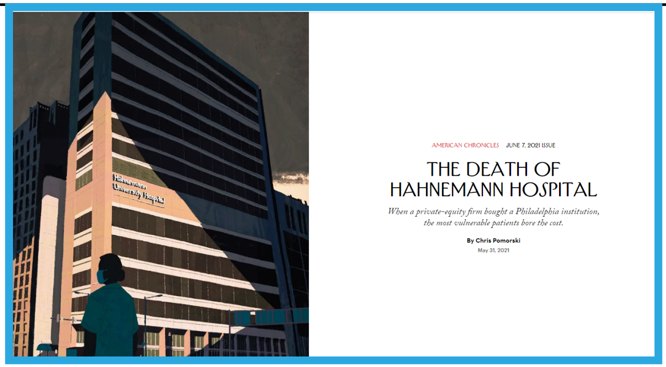
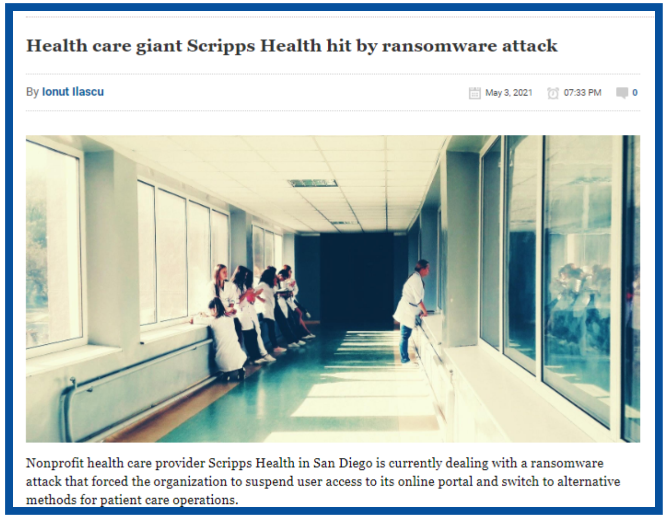
Data from Information Repositories (T0811) for Collection

- *Definition:* "Adversaries may target and collect data from information repositories" [MITRE ATT&CK for ICS]

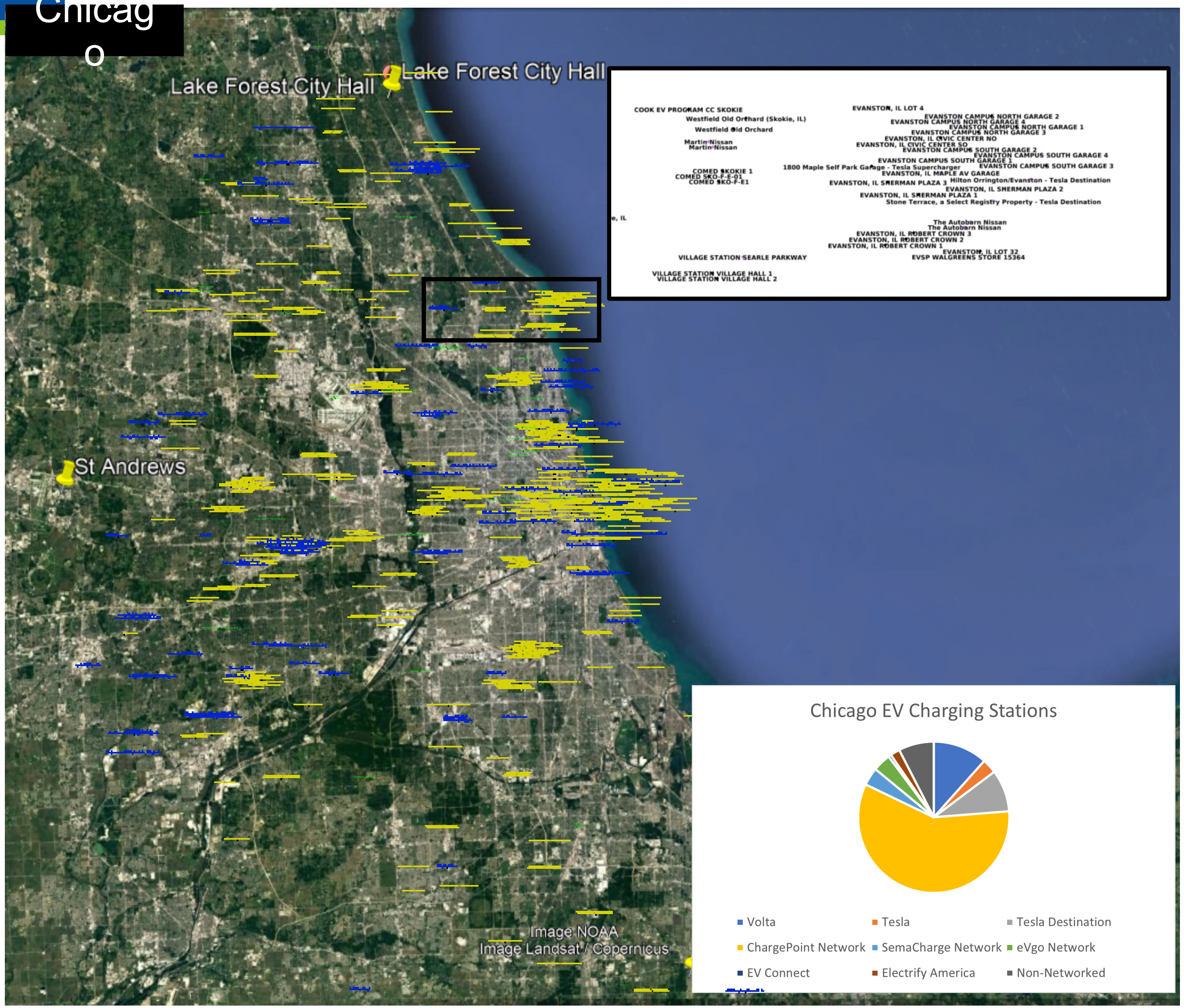
Social	 IEEE Spectrum Cops Tap Smart Streetlights Sp... Type to search NEWS SENSORS **Cops Tap Smart Streetlights Sparking Controversy and Legislation** › San Diego's sensor-laden streetlights were supposed to save money and inspire entrepreneurs. Then the police started using their cameras and the pushback began BY TEKLA S. PERRY | 08 AUG 2020 | 9 MIN READ	- *Approach:* Unexpected access to data via social relation between Police and City. - Video - CityIQ platform - *Impact:* - Inappropriate use of data - Reputation risk
Cyber	 Sections C4ISRNET Artificial Intelligence Unmanned Battlefield 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)	- *Approach:* Indirect data access via subsidiary or subcontractor - *Impact:* - Loss of Data

Loss of Availability (T0826) for Impact

- *Definition:* "Adversaries may attempt to disrupt essential components or systems to prevent owner and operator from delivering products or services" [MITRE ATT&CK for ICS]

Social	 AMERICAN CHRONICLES JUNE 7, 2021 ISSUE THE DEATH OF HAHNEMANN HOSPITAL *When a private-equity firm bought a Philadelphia institution, the most vulnerable patients bore the cost.* By Chris Pomorski May 31, 2021	• *Duration:* Permanent • *Impact:* • Loss of Data (patient records) • Loss of Education (residency) • Loss of Medical Care • Loss of Real Estate for Healthcare
Cyber	 Health care giant Scripps Health hit by ransomware attack By Ionut Ilascu May 3, 2021 07:33 PM 0 Nonprofit health care provider Scripps Health in San Diego is currently dealing with a ransomware attack that forced the organization to suspend user access to its online portal and switch to alternative methods for patient care operations.	• *Duration:* Four weeks to recover • *Impact:* • Loss of Availability • Re-routing of patients • Health outcomes (more cardiac events) • *Cost:* $113M

Loss of Availability: Electric Vehicle Charging Station Networks

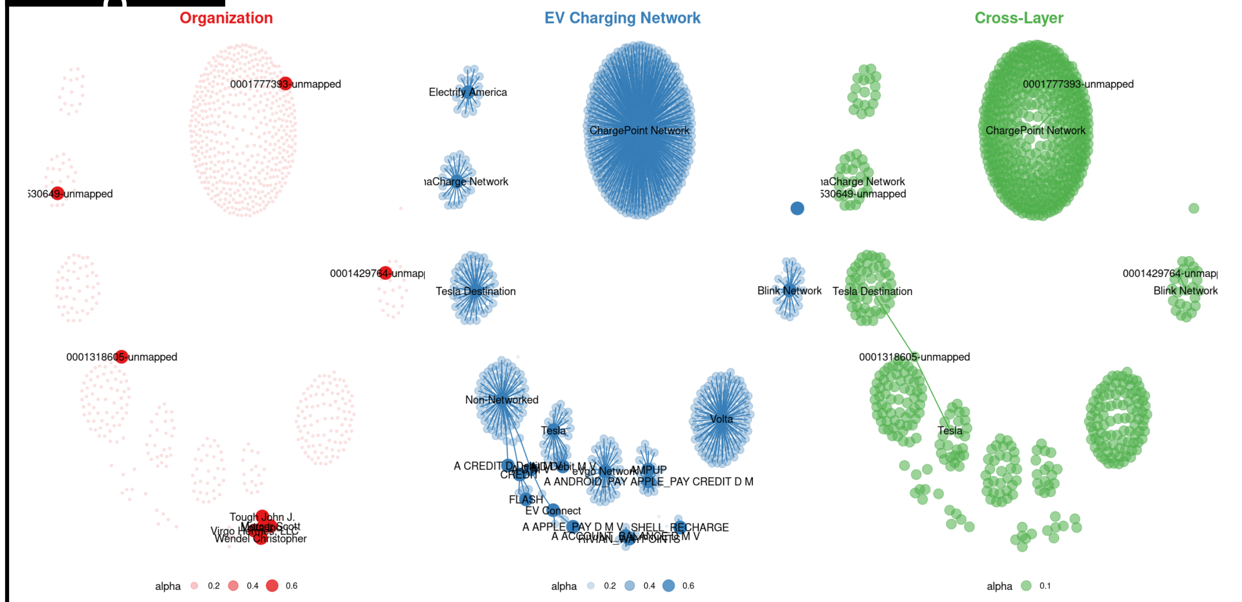

Chicag
o
Lake Forest City Hall
Lake Forest City Hall
St Andrews
COOK EV PROGRAM CC SKOKIE
Westfield Old Orchard (Skokie, IL)
Westfield Old Orchard
Martin Nissan
Martin Nissan
COMED SKOKIE 1
COMED SKO-F-E-01
COMED SKO-F-E1
e, IL
VILLAGE STATION SEARLE PARKWAY
VILLAGE STATION VILLAGE HALL 1
VILLAGE STATION VILLAGE HALL 2
EVANSTON, IL LOT 4
EVANSTON CAMPUS NORTH GARAGE 2
EVANSTON CAMPUS NORTH GARAGE 4
EVANSTON CAMPUS NORTH GARAGE 1
EVANSTON CAMPUS NORTH GARAGE 3
EVANSTON, IL CIVIC CENTER NO
EVANSTON, IL CIVIC CENTER SO
EVANSTON CAMPUS SOUTH GARAGE 2
EVANSTON CAMPUS SOUTH GARAGE 4
EVANSTON CAMPUS SOUTH GARAGE 1
1800 Maple Self Park Garage - Tesla Supercharger
EVANSTON CAMPUS SOUTH GARAGE 3
EVANSTON, IL MAPLE AV GARAGE
EVANSTON, IL SHERMAN PLAZA 3
Hilton Orrington/Evanston - Tesla Destination
EVANSTON, IL SHERMAN PLAZA 2
EVANSTON, IL SHERMAN PLAZA 1
Stone Terrace, a Select Registry Property - Tesla Destination
The Autobarn Nissan
The Autobarn Nissan
EVANSTON, IL ROBERT CROWN 3
EVANSTON, IL ROBERT CROWN 2
EVANSTON, IL ROBERT CROWN 1
EVANSTON, IL LOT 32
EVSP WALGREENS STORE 15364
Image NOAA
Image Landsat / Copernicus
Chicago EV Charging Stations
Volta
Tesla
Tesla Destination
ChargePoint Network
SemaCharge Network
eVgo Network
EV Connect
Electrify America
Non-Networked

Geospatial Attributes

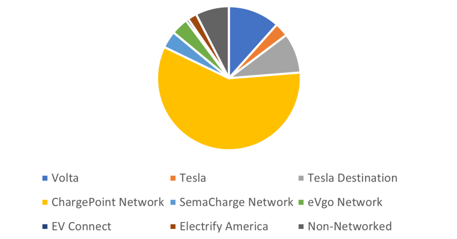
- Enables the ability to zoom in on a given region of interest and see who has influence and where
  - ChargePoint
  - Volta
  - eVgo
- Data Sources:
  - SEC EDGAR
  - DOE Alt. Fuels Database

Regional Comparison of EV Charging Station Vendors

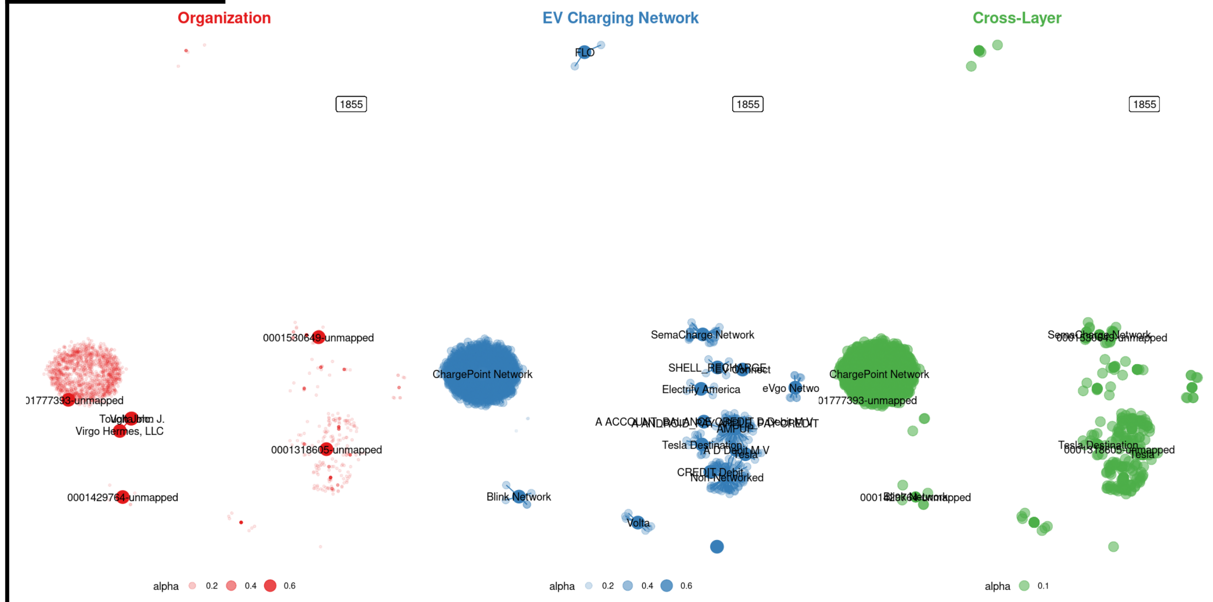
Chicag o



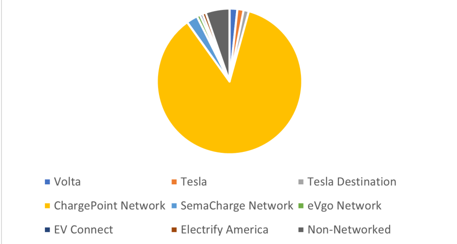
Chicago EV Charging Stations



Boston



Boston EV Charging Stations



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.

INL

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.

WWW.INL.GOV