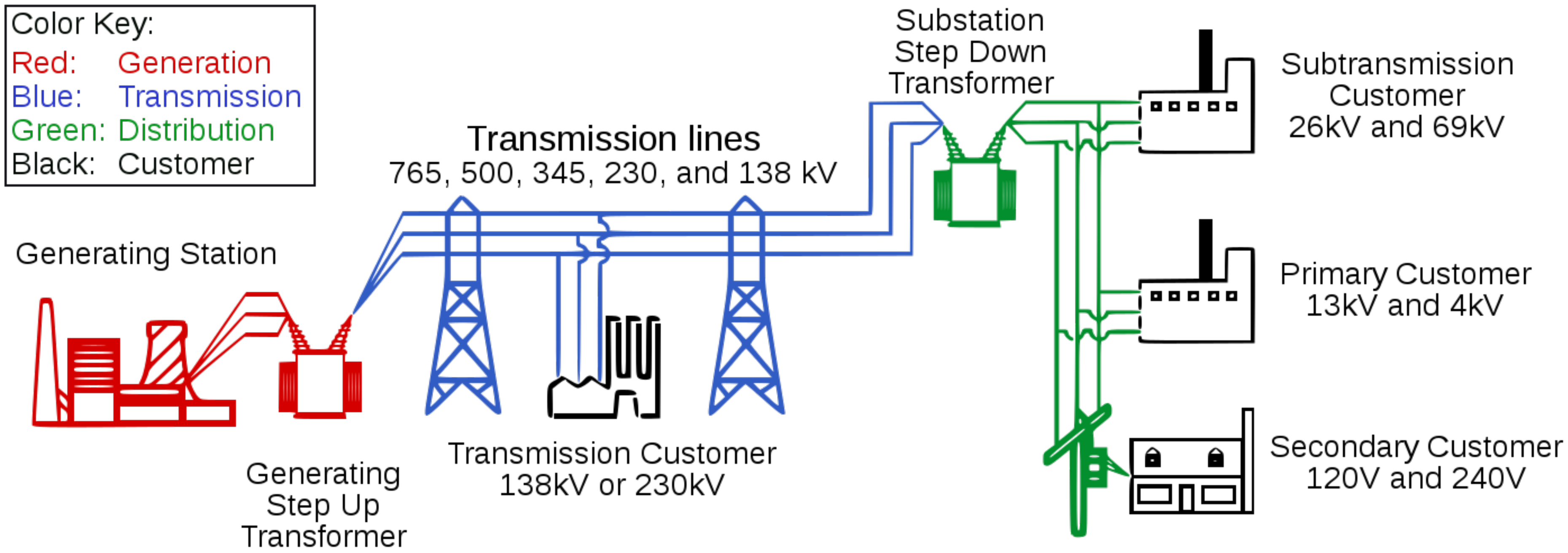
Economics of Grid-Edge Cyber Resiliency

Yury Dvorkin
NYU → JHU
@yury_dvorkin

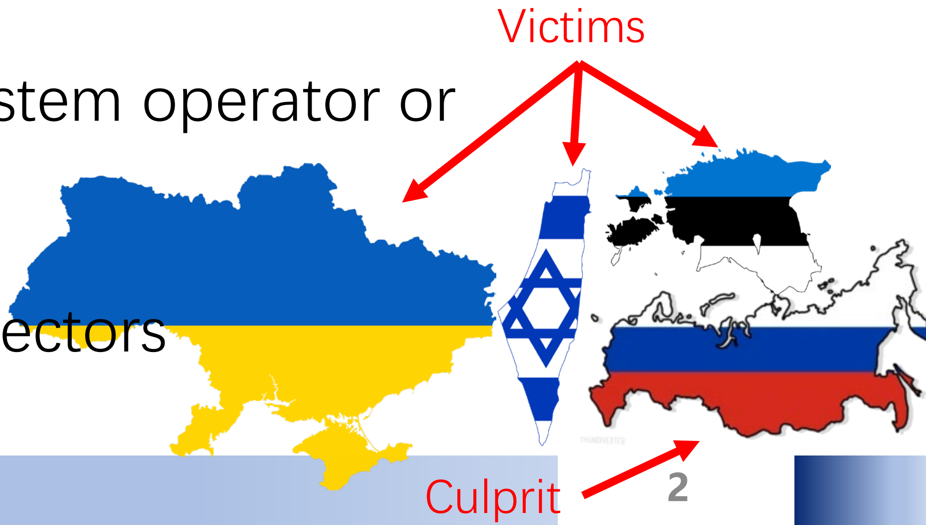
NYU | TANDON SCHOOL OF ENGINEERING
JOHNS HOPKINS RALPH O'CONNOR SUSTAINABLE ENERGY INSTITUTE
JOHNS HOPKINS WHITING SCHOOL of ENGINEERING

Electric Power Distribution



24/7/365 operational cycle:

- Centralized industry-grade control systems (e.g. system operator or utility, substations, power plants)
- Industry-grade cyberdefense
- Lots of ***direct*** and ***already weaponized*** attack vectors



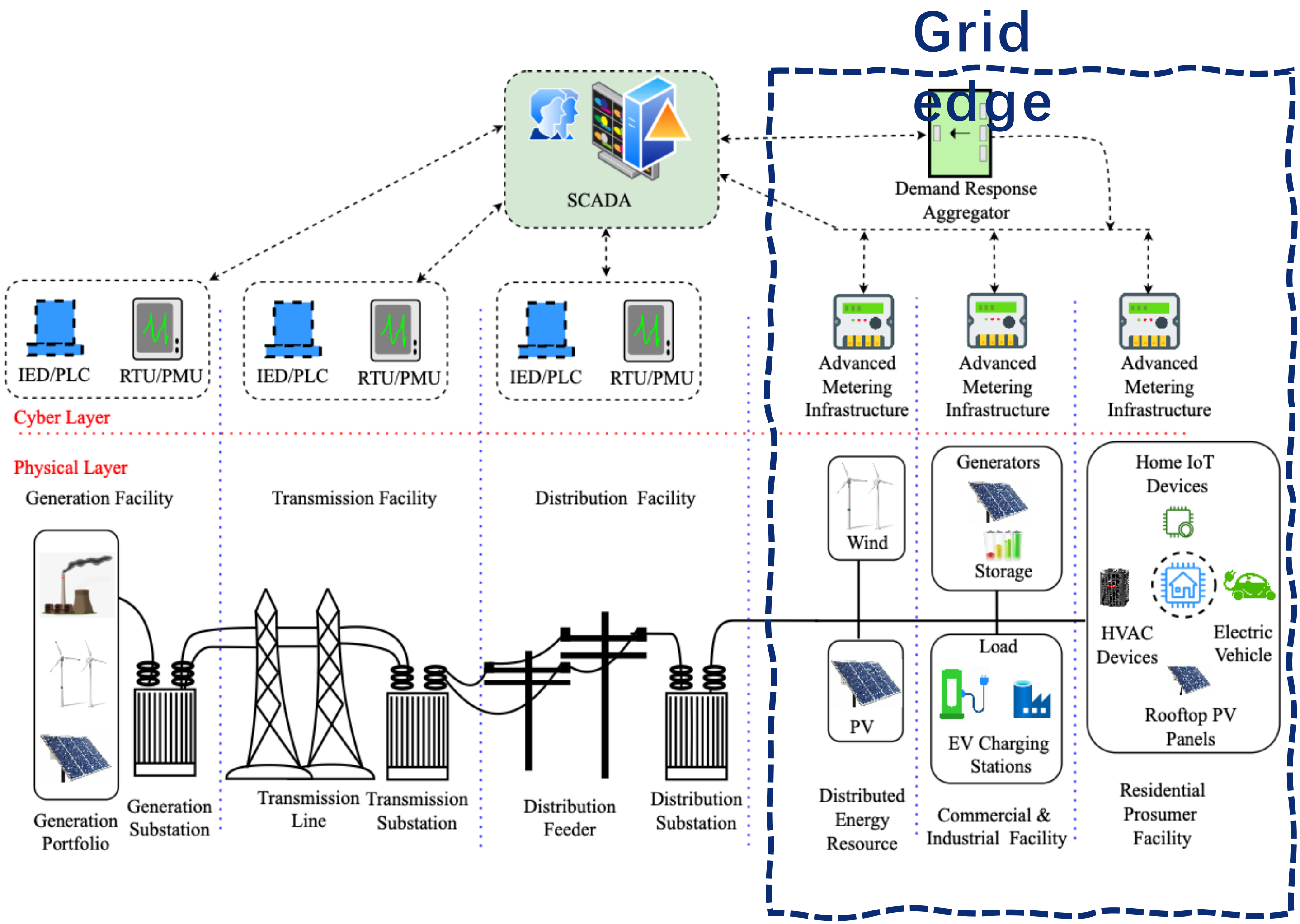
What Is Grid Edge?

Grid edge does not have a clear definition and the line is blurry

- Behind-the-meter assets
- Third-party assets, even if SCADA-interfaced
- Some decentralization and autonomy

Sometimes it is easier to name and exclude grid assets

- Utility- and SCADA-interfaced assets

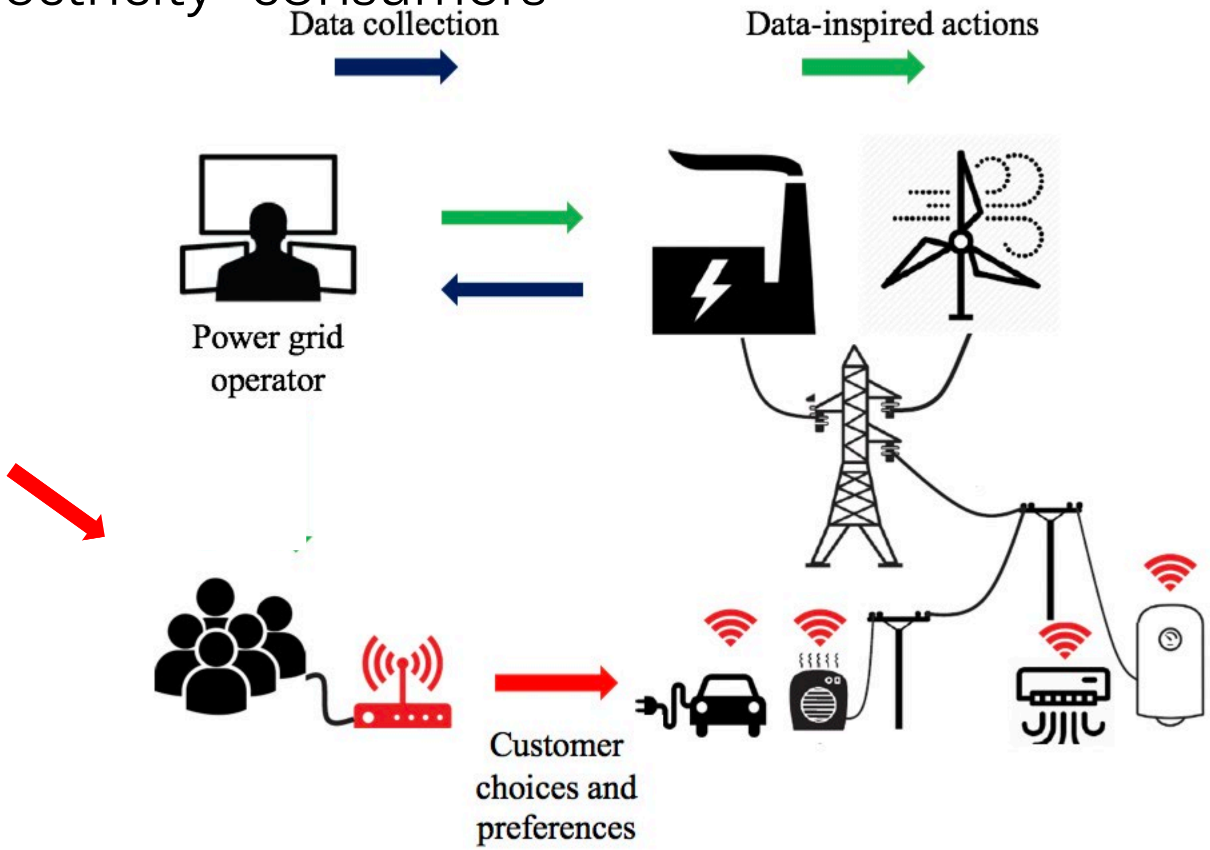


Weaponizing Grid Edge Attack Vectors

Grid edge is exposed to ***indirect*** *attack vectors:*

- Low security awareness/hygiene among electricity consumers
- No industry-grade cyber defense
- Many novel attack angles
- Stealthy to the utility

Attacker



Many unknown effects:

- New objectives (e.g. adversarial learning)
- “Human-in-the-loop” factors
- Ability to scale and self-reproduce

Grid-Edge Cyber Risks: Different Perspectives

BlackIoT: IoT Botnet of High Wattage Devices Can Disrupt the Power Grid

Saleh Soltan, Prateek Mittal, and H. Vincent Poor, *Princeton University*

https://www.usenix.org/conference/usenixsecurity18/presentation/soltan

Not Everything is Dark and Gloomy: Power Grid Protections Against IoT Demand Attacks

Bing Huang, *The University of Texas at Austin;* Alvaro A. Cardenas, *University of California, Santa Cruz;* Ross Baldick, *The University of Texas at Austin*

https://www.usenix.org/conference/usenixsecurity19/presentation/huang

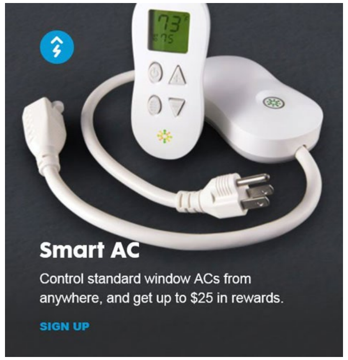
An important outcome of Huang et al:

- Grid-edge attacks are likely to be contained in distribution/sub-transmission networks
- Grid impacts are highly sensitive to an exploited attack vector

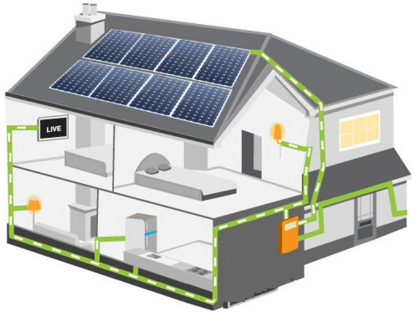
All Attack Vectors Are Equal, But Some ...

Attack Sophistication

EVs



DR programs



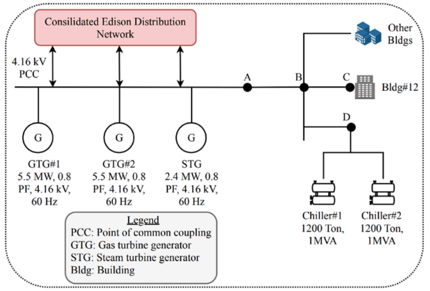
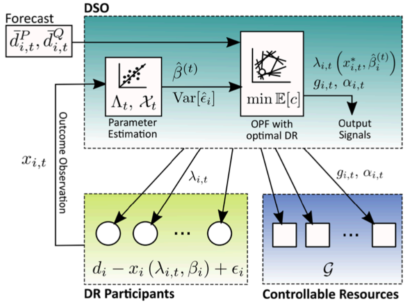


Figure 11. Schematic diagram of NYU microgrid depicting combined heat and power generation [95], where AB, BC, and BD are distribution lines modeled in the CC-OPF implementation.

Micro, nano, pico-grids



Decentralized decision systems

Attack Impact

An Quick Look Into Economics Of Grid-Edge Cyber Resiliency

Grid-edge actors have a complex loss surface:

- Not exposed to the cost of power outages
- Not exposed to regulatory and compliance risks

- Exposed to profit opportunity losses
- Exposed to damage costs

Charging & Profit losses:

- 1 EV @ 250 kW in 20 min
- $20 per full charge
- Profit loss per stall - **$60/hr**
- 4 stalls = 1 MWh of charging loss = **$240/hr**

Cost of power outages:

- VOLL is $11-**60,000/MWh**

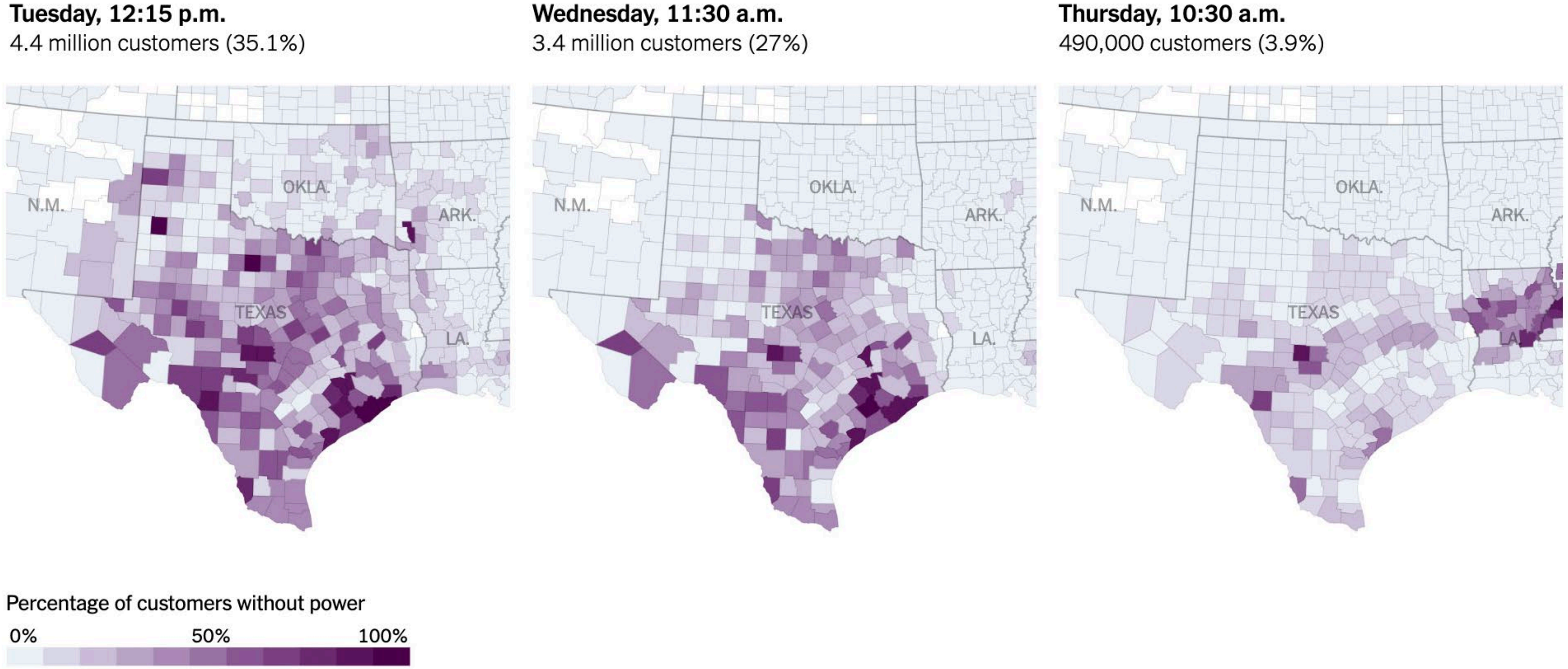
Social vs private risk exposures are grotesquely misaligned (45-250 times!)

Looks Familiar?

Think of the Feb 2021 disaster in TX (a poster child for private vs social risk imbalances)

- A lack of investment in weather resiliency
- Surplus of online producers has, in fact, increased due to scarcity
- Non-opportunity losses of offline producers has been $22m (est)

Similarity to grid-edge cyber resiliency via a **missing incentive** problem



The Rest of This Presentation

How to solve a missing incentive problem to promote grid-edge cybersecurity?

We will follow the lessons learned thus far:

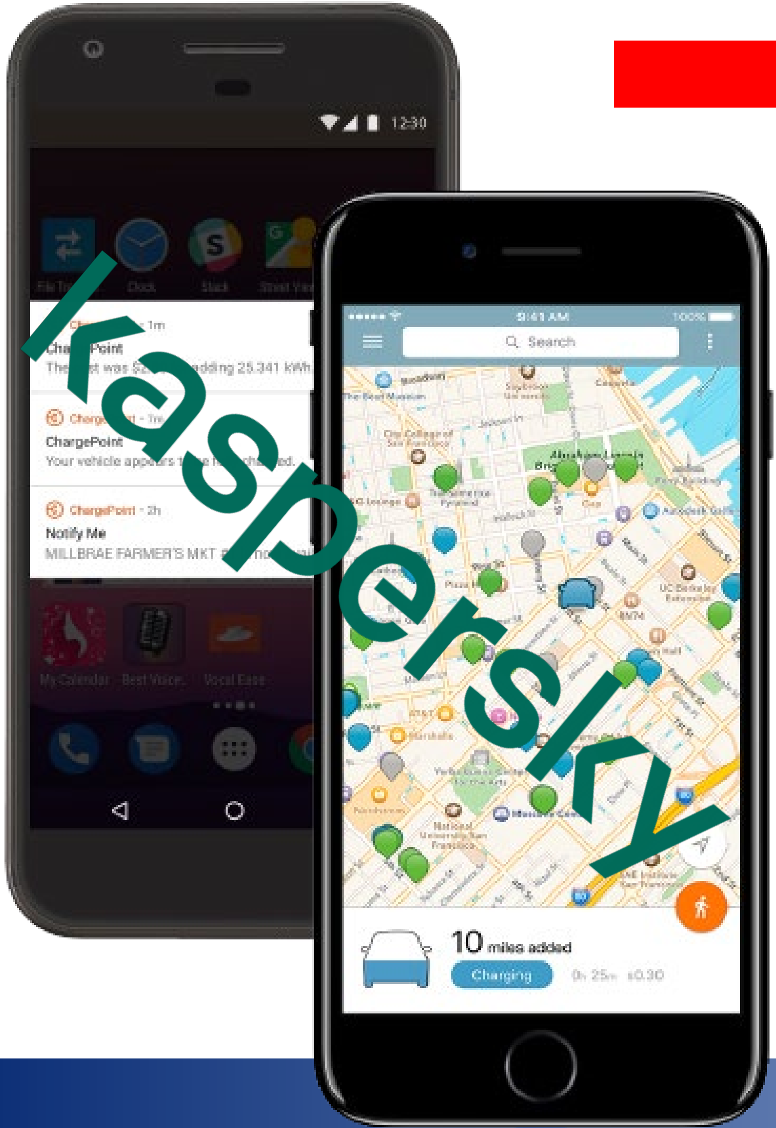
- Huang et al: Focus on EV-specific attack vectors and distribution network impacts
- Compliance: lightweight solutions which requires minimal regulatory approvals

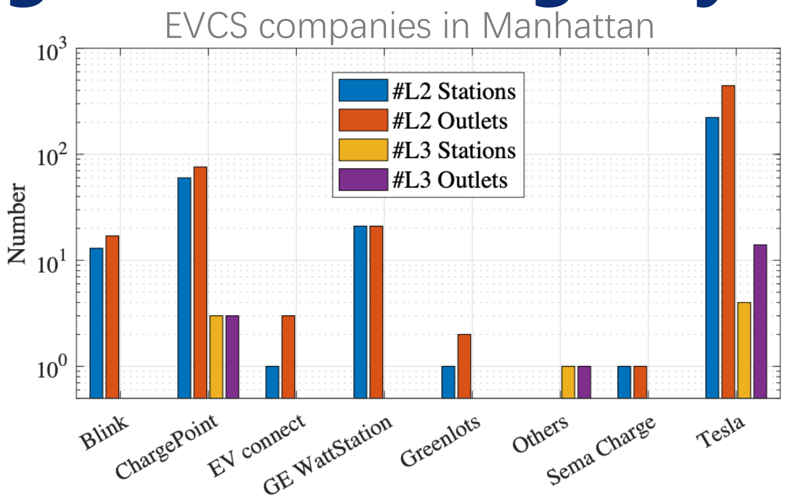
Solution (sketch):

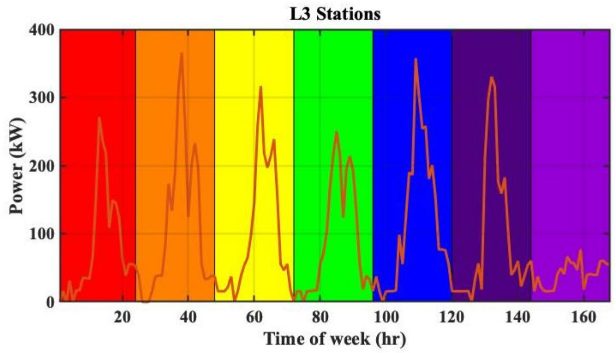
- Introduce a cyber insurance mechanism that shares social/system risks with private actors (EV charging stations)
- Relate it to a business model of the EV charging station operators
- Leverage cyber insurances to promote better cyber security compliance

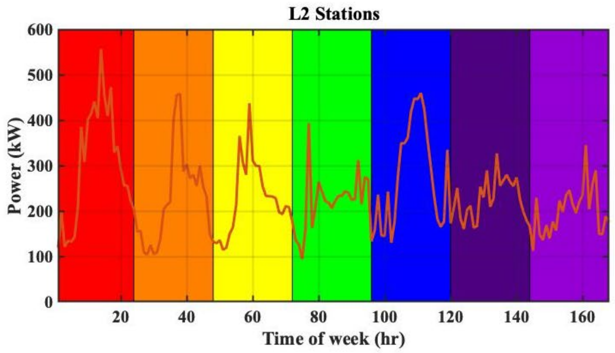
Origins of EV Charging as a Grid-Edge Cyber Threat

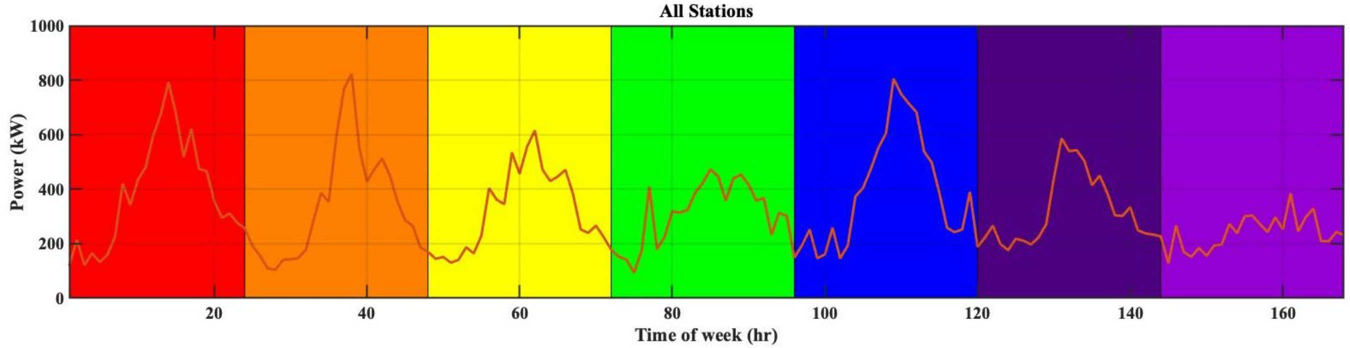
Where do we get EV data?









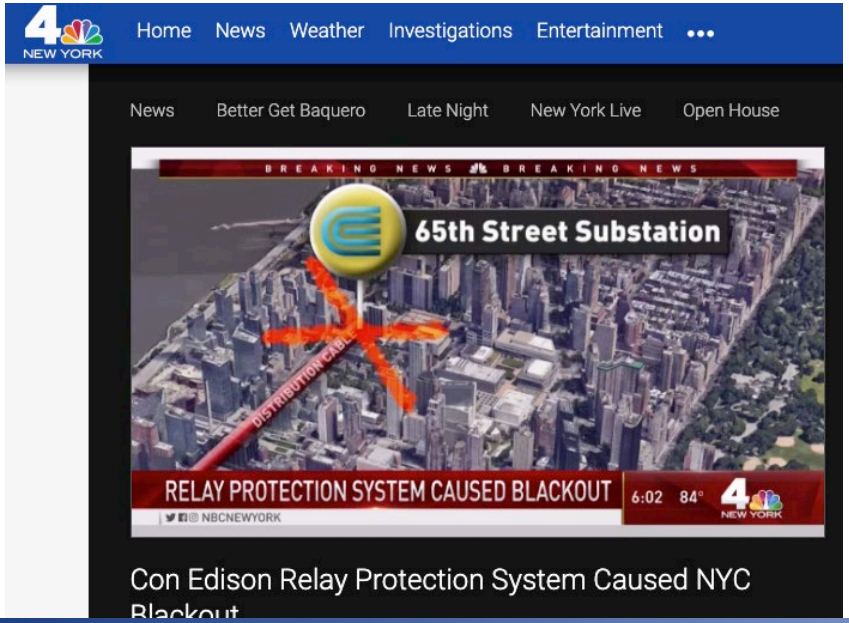


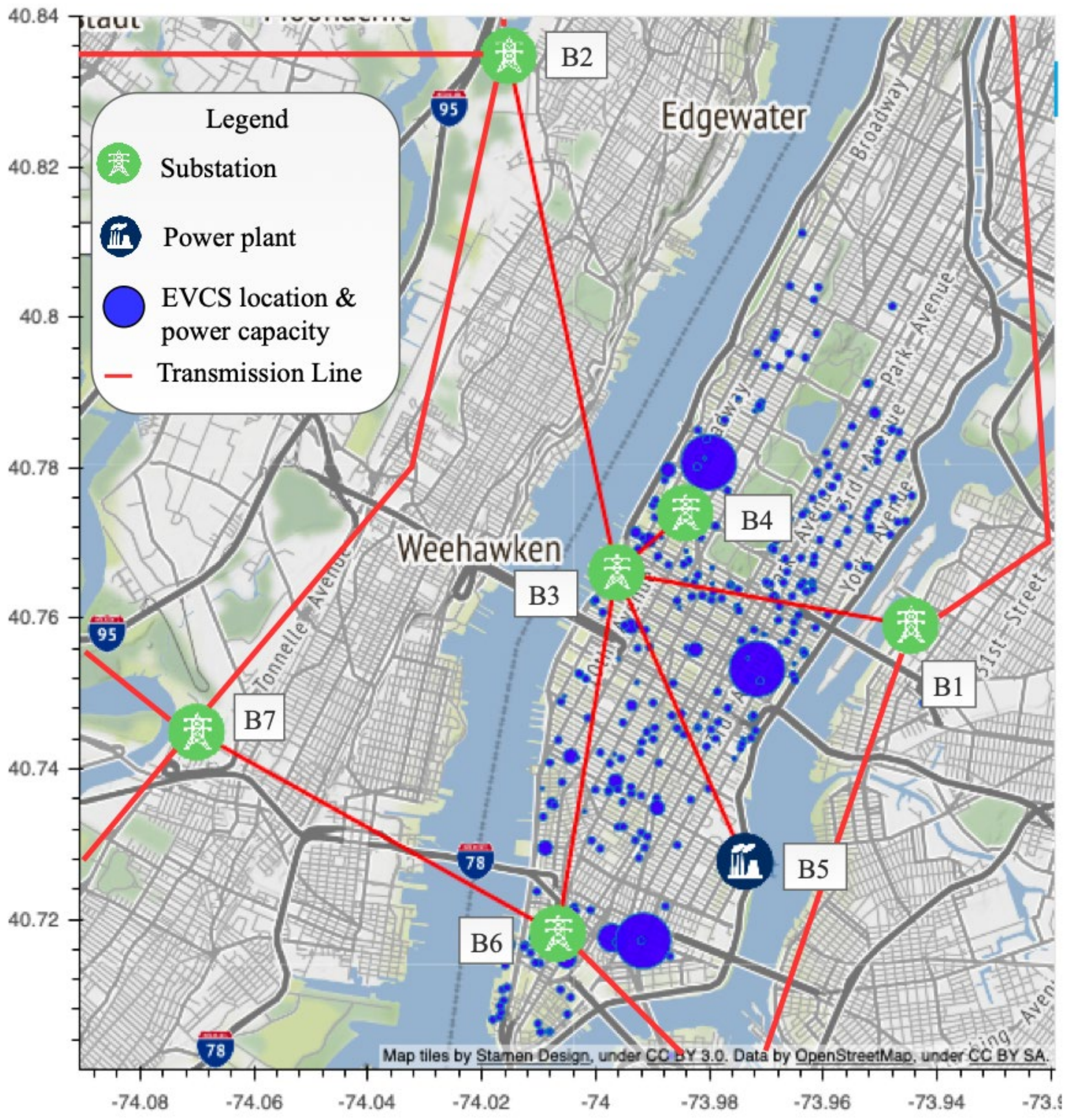
We got all the EV data we need!

Origins of EV Charging as a Grid-Edge Cyber Threat

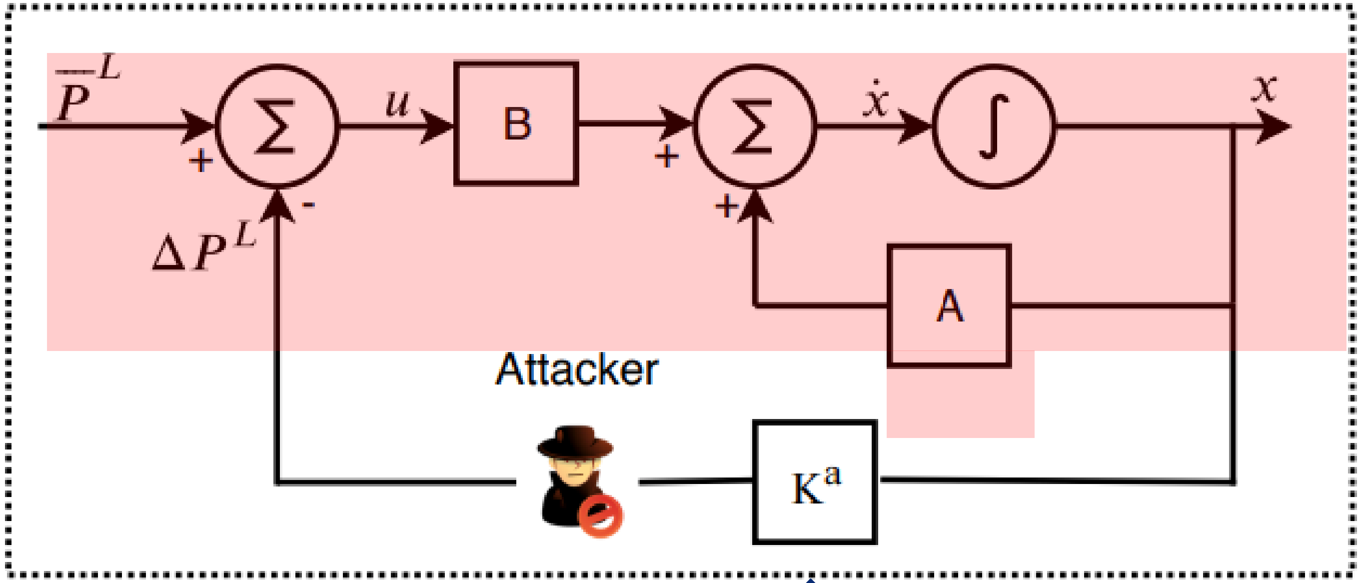
Where do we get grid data?

- Google Maps
- IEEE
- Con Edison
- NYISO
- US EIA
- Reports, public releases, news reporting, e





Even A Conservative Attack on EV Charging Will Make Front Pages



Well-known power grid models & estimated parameters

Using the data, we take the perspective of the attacker and design a remote, state-feedback-based, data-driven attack strategy

300-1000 x 

are needed to cause a brown/blackout on Manhattan, NY

How to Design an Insurance Mechanism?

Insurer

$$\min x$$
$$s.t. \quad x \geq \underbrace{f1\left(\mathcal{P}(A), \gamma, \kappa, r, A_h\right)}_{\text{Policy factors}} * \underbrace{f2(d, \lambda^{c,*})}_{\text{EVCS revenue}}$$

EV charging price (λ^c),
EVCS demand forecast (d),
Co-insuarnce factor (γ)

EVCS operator

$$\lambda^c \in \arg\min g1(\lambda^c)$$
$$s.t. \quad \underbrace{C(\lambda^c, \lambda^u, x^*, d, \gamma, \mathcal{P}(A))}_{\text{Net EVCS operating cost}} \leq 0$$

Premium (x)

Policy Factors	Symbol
Profit loading factor	r
Penalty for attack history	κ
Co-insurance factor	γ
Probability of attack on the EVCS	$P(A)$

This bi-level optimization can be solved **analytically**:

$$x^* = \frac{C}{[(\mathbb{P}(A)(\gamma-1)+1)-C]}\left[\mathbb{P}(A)\rho\sum_t D_t + (1-\mathbb{P}(A))\sum D_t \lambda_t^{u,*}\right],$$

A More Challenging Case with Dynamic Electricity Tariffs

$$\min x$$
$$s.t. \quad x \geq f1 \underbrace{(\mathcal{P}(A), \gamma, \kappa, r, A_h)}_{\text{Policy factors}} * \underbrace{f2(d, \lambda^{c,*})}_{\text{EVCS revenue}}$$

EV charging price (λ^c),
EVCS demand forecast (d),
Co-insuarnce factor (γ)

Insurer

$$\lambda^c \in \arg\min g1(\lambda^c)$$
$$s.t. \quad \underbrace{C(\lambda^c, \lambda^u, x^*, d, \gamma, \mathcal{P}(A))}_{\text{EVCS cost}} \leq 0$$

Premium (x)

Dynamic electricity price (λ^u)

EVCS operator

$$\lambda^u \in \underbrace{C(g, c^g)}_{\text{Grid operating cost}}$$
$s.t.$ Power flow equations with d

EVCS demand forecasts (d)

Power grid operator

This tri-level optimization is solved **numerically, but optimally** using column-and-cut generation algorithm.

Data is Crucial to Internalize Risks Into Insurance Design

- The insurance design depends upon EV charging demand forecasts.
- The EVCS power demand forecasts can have errors
- There is a risk in choosing a forecast to calculate the premium and EVCS cost.
- Conditional Value-at-Risk (CVaR) metric is used to quantify this risk.

EVCS demand forecast (d)

$$\lambda^c \in \arg\min g1(\lambda^c)$$
$$s.t. \quad \underbrace{C(\lambda^c, \lambda^u, x^*, d, \gamma, \mathcal{P}(A))}_{\text{EVCS cost}} \leq 0$$

EVCS operator

EVCS demand forecast (d)

Data is Crucial to Internalize Risks Into Insurance Design

We **robustify** insurance design against uncertainty in **real-world** data

Parameter	Symbol	Actions
Profit loading factor	r	Box constrains informed by industry practices
Penalty for attack history	κ	
Co-insurance factor	γ	
Probability of attack	$P(A)$	Data-driven Semi-Markov process (SMP)

$$\boxed{\text{Attack data on IT sector}} \rightarrow \boxed{\text{SMP}} \rightarrow P(A)$$

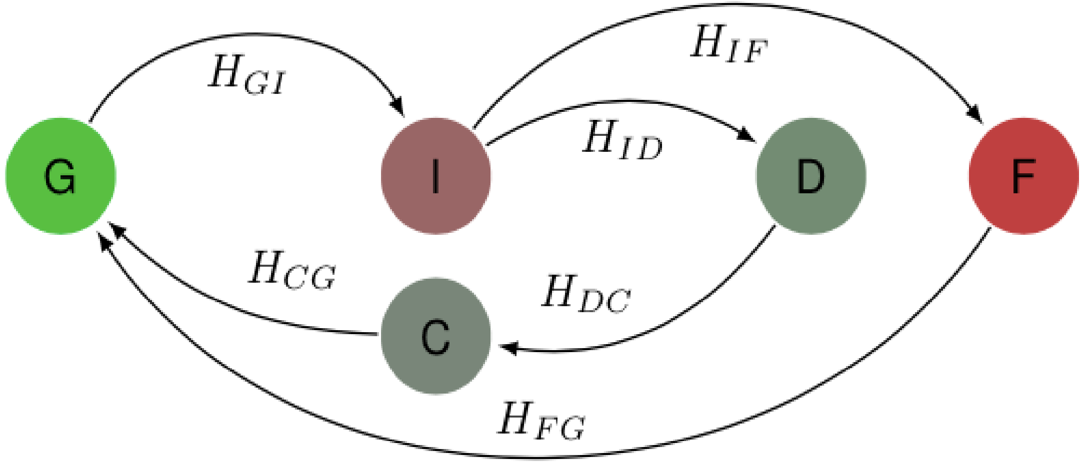
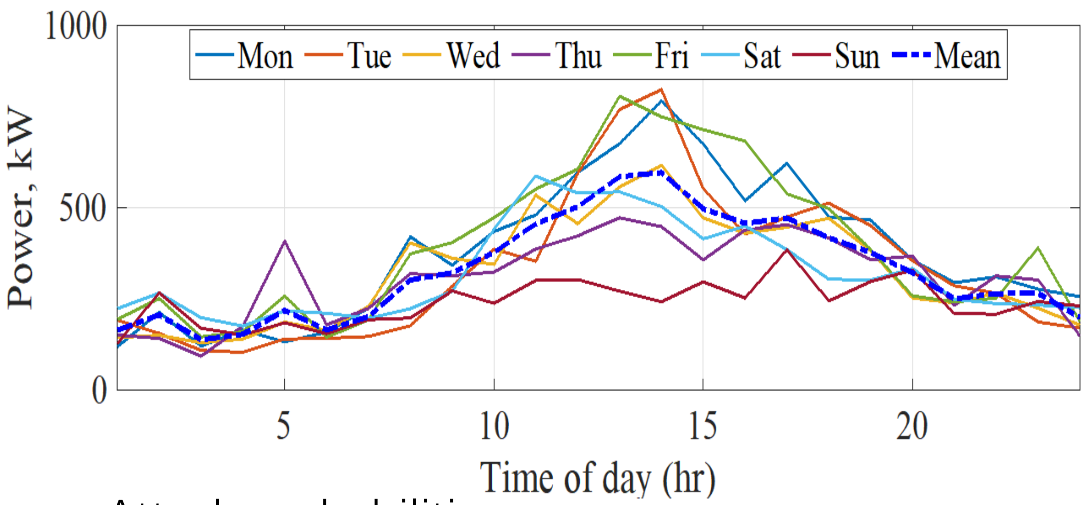


Fig: Semi-Markov Process (SMP) for cyberattacks on EVCSs. H(·) defines the Cumulative Distribution Function (CDF) of the state transition time.

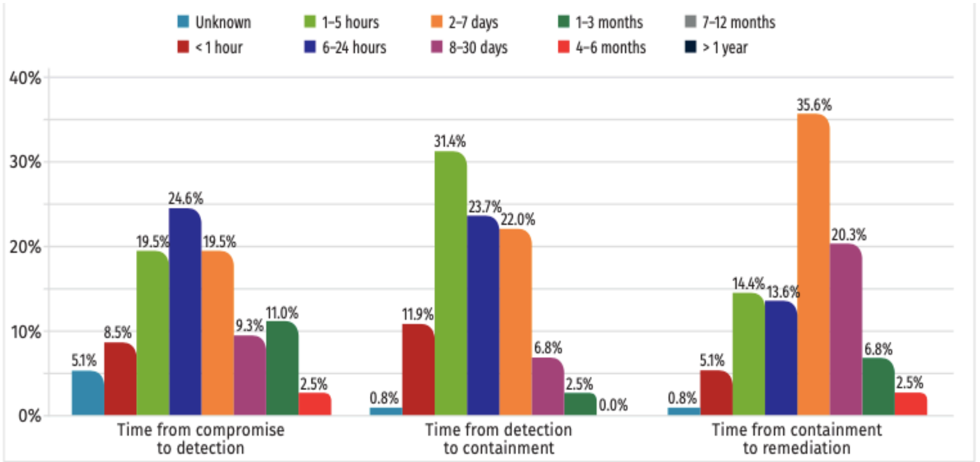
Symbol	Name of the state
G	Good
I	Intrusion
D	Detection
C	Containment
F	Failure

Insurance Premium is Very Sensitive to Parameters

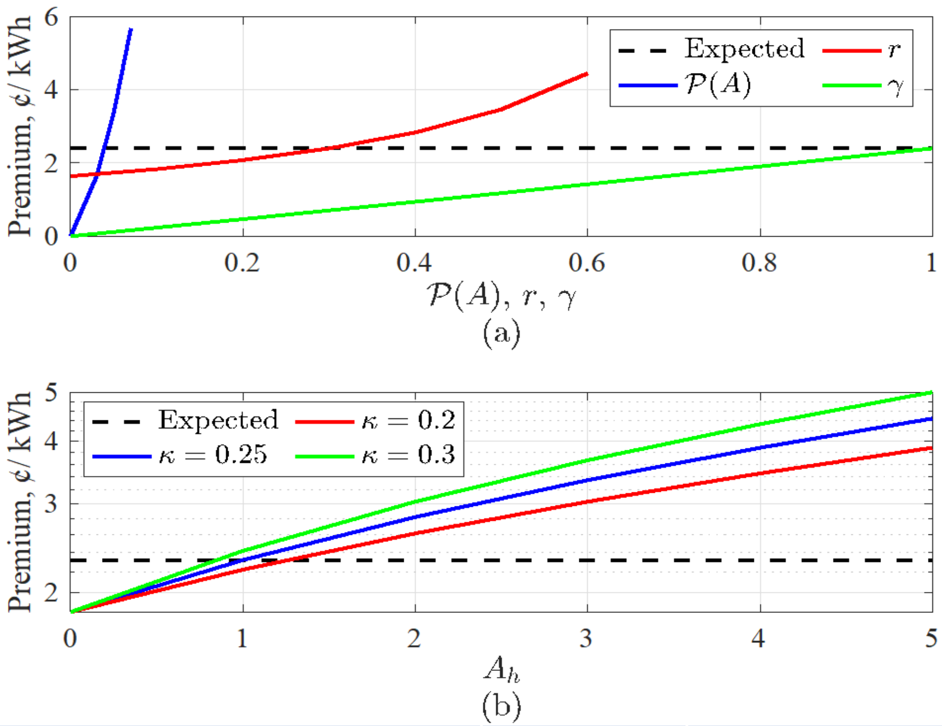
- EVCS demand uncertainty



- Attack probabilities



Note to my future self: this **data varies** locationally a lot! Whatever works for NYC, may not work for Israel, Estonia and Ukraine.



Parameter	Symbol	Sensitivity
Probability of attack	$P(A)$	Most sensitive (almost exponential)
Profit loading factor	r	Linear up to a point then a swift change
Co-insurance factor	γ	Linear
Penalty for attack history	κ	Log-linear
Number of attacks in the past	A_h	Log-linear

Robust Insurance Design

- Upper bounds are set by the upper limit of the uncertain parameters.
- Lower bounds are set by the lower limit of the uncertain parameters.
- Expected value is set by the average value of the uncertain parameters.
- Insurance premium and EV charging price **increase** with **the risk-attitude of the EVCS**.

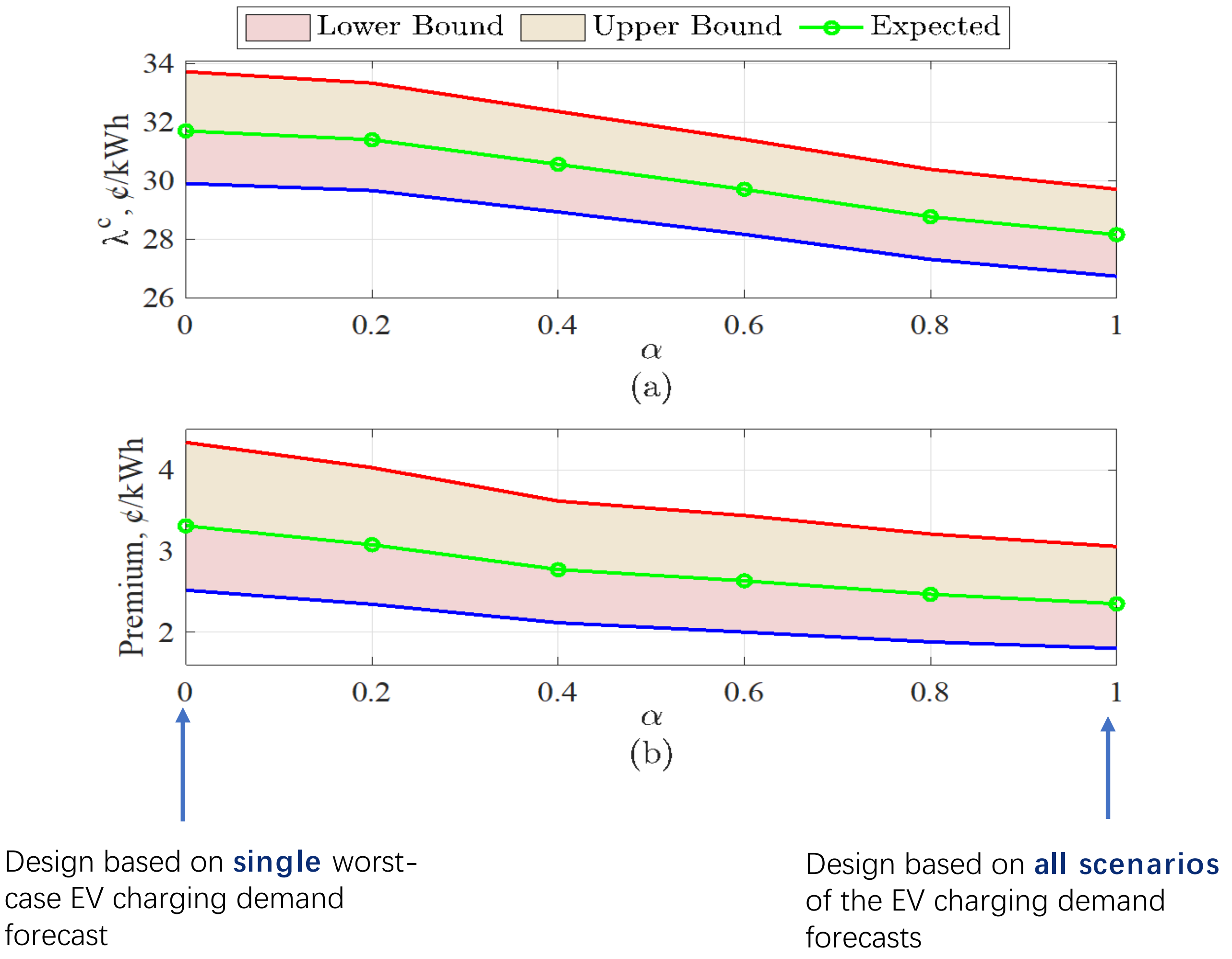


Fig: Risk-Averse and robust EV charging prices and cyber insurance premiums.

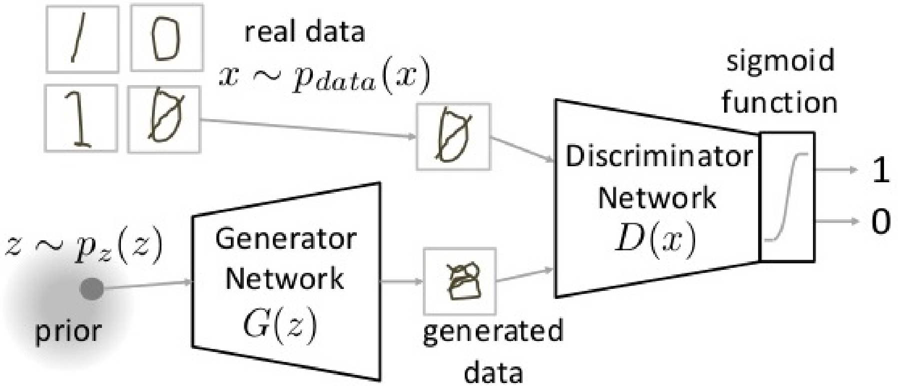
Grid-Edge Cyber Resiliency and Autonomy

- Grid edge enables autonomy via a high degree of decentralized decision-making
  - Compromised grid-edge assets is a system risk due to untrustworthy autonomy
- Grid-edge cyber risks are easily, in theory, solved if framed as a missing incentive problem (not necessarily as an insurance design problem), but
  - Availability of high-fidelity data is a major setback
  - Privacy restrictions fueled by decentralization and autonomy exacerbate data challenges for insurance design

Concluding Thoughts for Grid-Edge Cyber Resiliency

- "Ask what you can do for your country"
  - Develop incentives to maintain & promote cybersecurity at the edge
  - More instruments for risk-sharing between the grid and customers
  - Smart and flexible regulatory environment and product certification
    - Very difficult to find one solution for 50 states
  - Customer education and engagement via outreach

- Emerging risks:
  - GAN-based make data-driven, model-free attack representations possible (a.k.a. Deepfakes)
  - Data requirements for attack execution will reduce in the future



References

1. S. Acharya, R. Mieth, R. Karri, and Y. Dvorkin, “False Data Injection Attacks on Data Markets for Public Electric Vehicle Charging Stations,” *Applied Energy,* 2022.
2. S. Acharya, R. Mieth, C. Konstantinou, R. Karri, and Y. Dvorkin, “Cyber Insurance Against Cyberattacks on Electric Vehicle Charging Stations,” *IEEE Transactions on Smart Grid*, 2022.
3. S. Acharya, Y. Dvorkin, R. Karri “Causative Cyberattacks on Online Learning-based Automated Demand Response Systems” *IEEE Transactions on Smart Grid*, 2021.
4. R. Mieth, S. Acharya, A. Hassan and Y. Dvorkin, “Learning-enabled Residential Demand Response”, *IEEE Electrification Magazine*, 2021.
5. S. Acharya, Y. Dvorkin, H. Pandzić, and R. Karri “Cybersecurity of Smart Electric Vehicle Charging: A Power Grid Perspective,” *IEEE Access*, 2020.
6. S. Acharya, Y. Dvorkin, R. Karri, “Public Plug-in Electric Vehicles + Grid Data: Is a New Cyberattack Vector Viable?,” *IEEE Transactions on Smart Grid*, 2020.

Thank you!

@yury_dvorkin





Leader: Samrat Acharya (Ph.D'22)
Next stop: PNNL