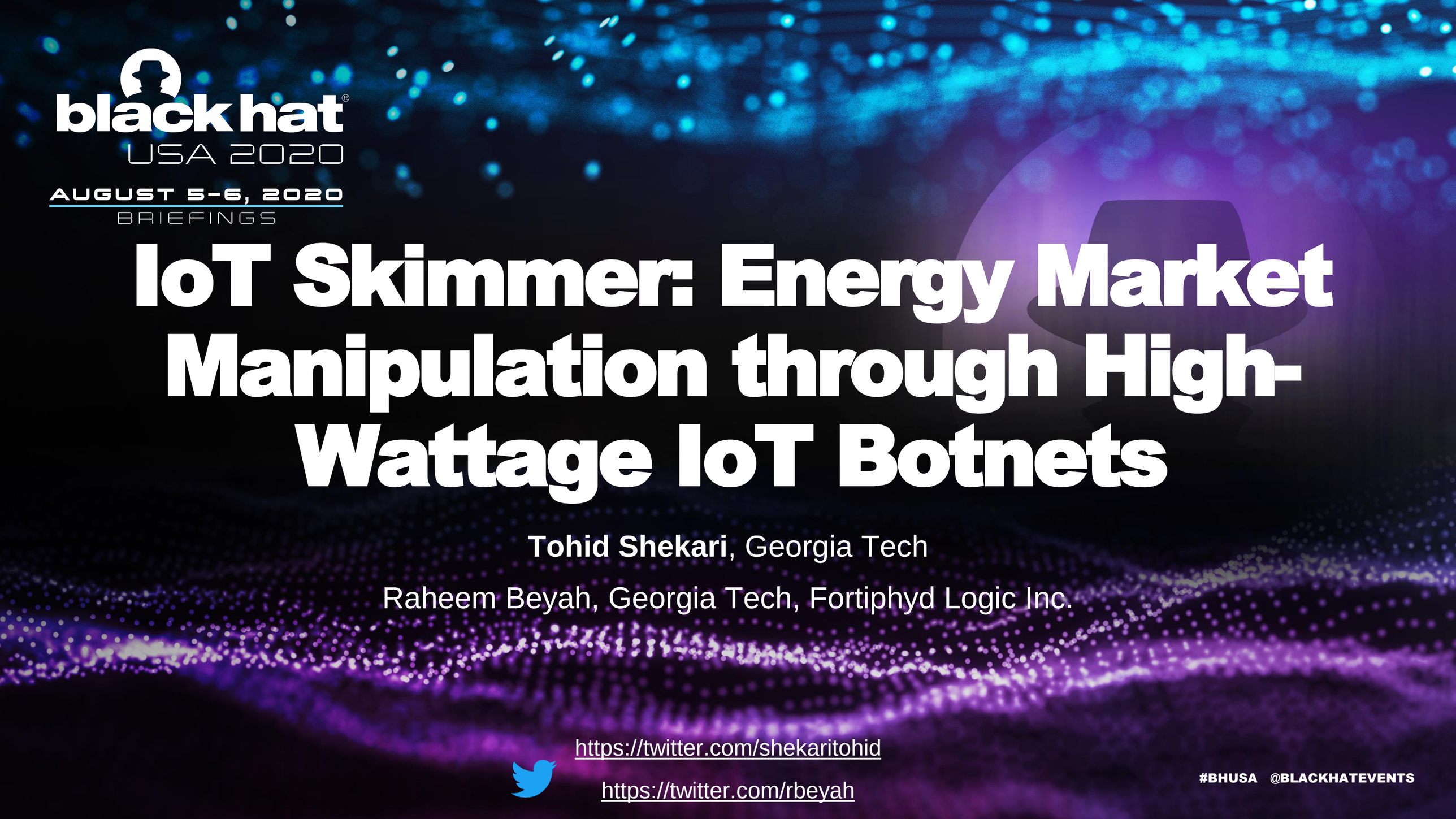



# IoT Skimmer: Energy Market Manipulation through High-Wattage IoT Botnets

**Tohid Shekari**, Georgia Tech

Raheem Beyah, Georgia Tech, Fortiphyd Logic Inc.

https://twitter.com/shekaritohid

https://twitter.com/rbeyah

# IoT Skimmer Team

COMMUNICATIONS ASSURANCE & PERFORMANCE GROUP

Georgia Tech

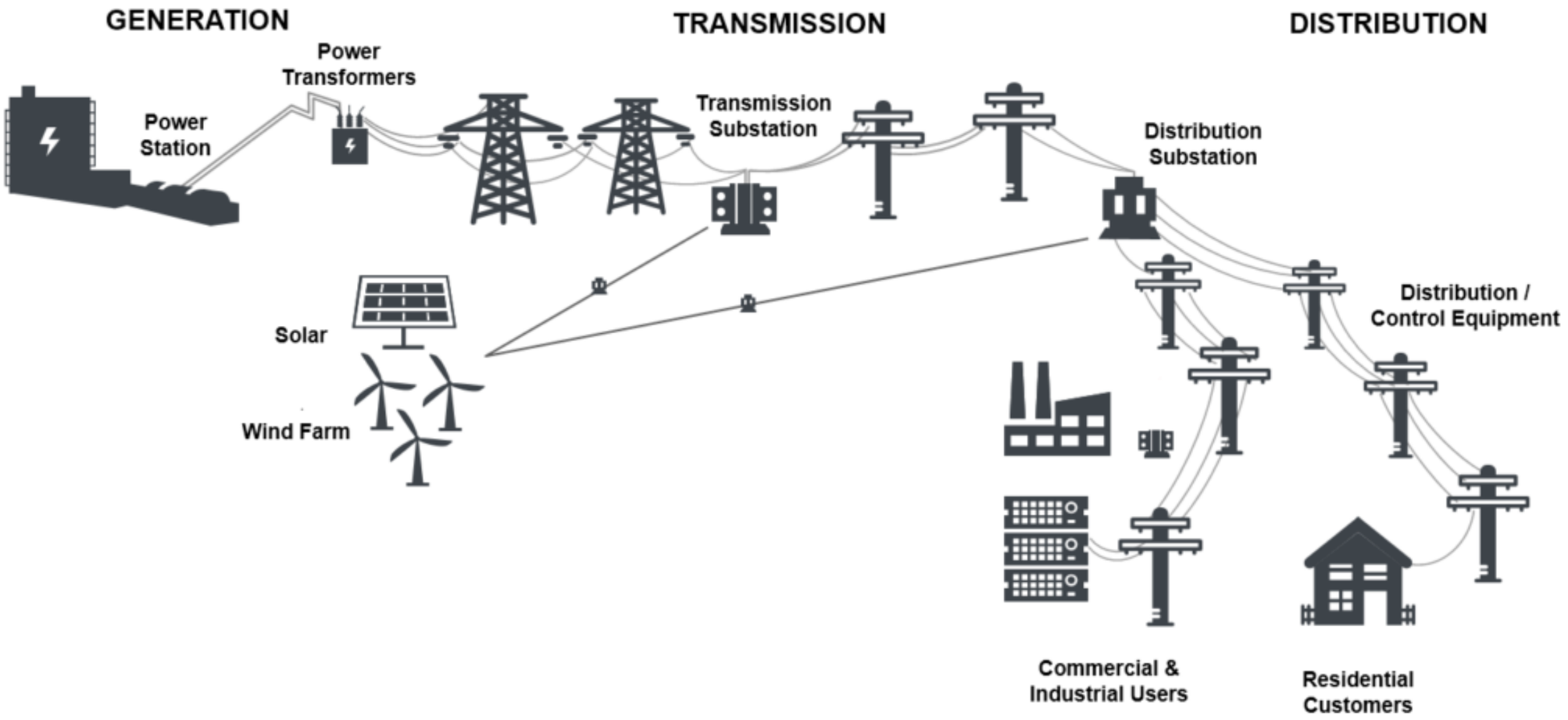
**Tohid Shekari**
PhD Candidate

**Celine Irvene**
PhD Candidate

**Raheem Beyah**
Professor

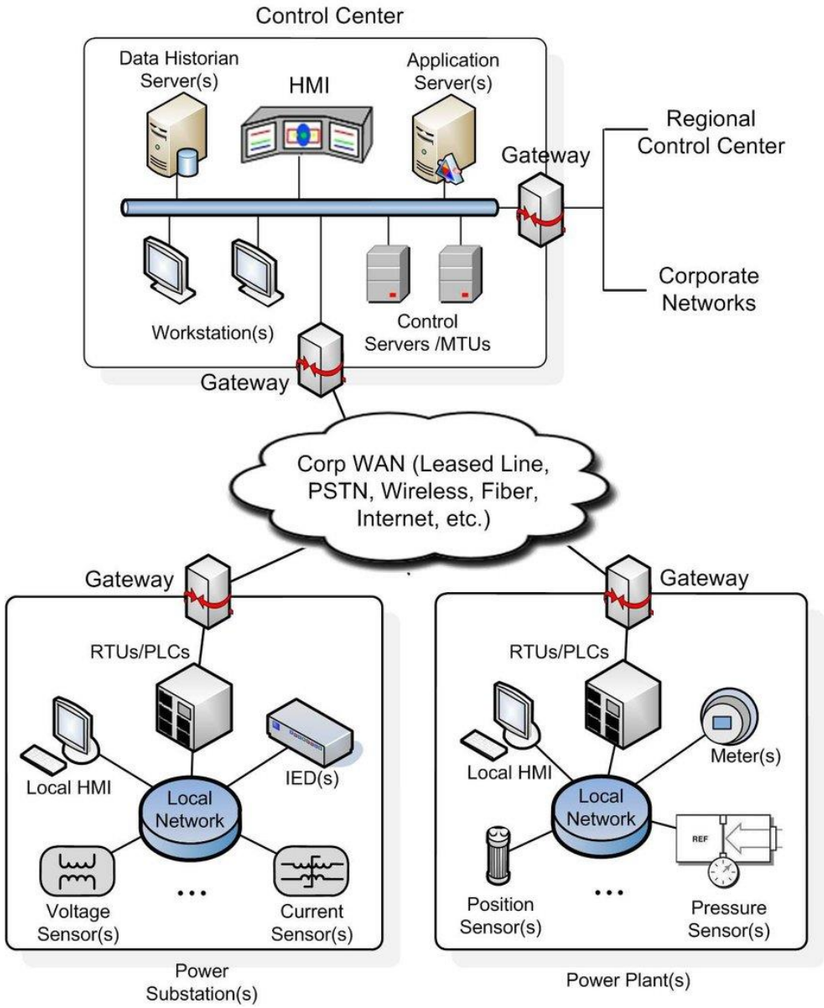
# Background – Power Grid

- Power grid structure



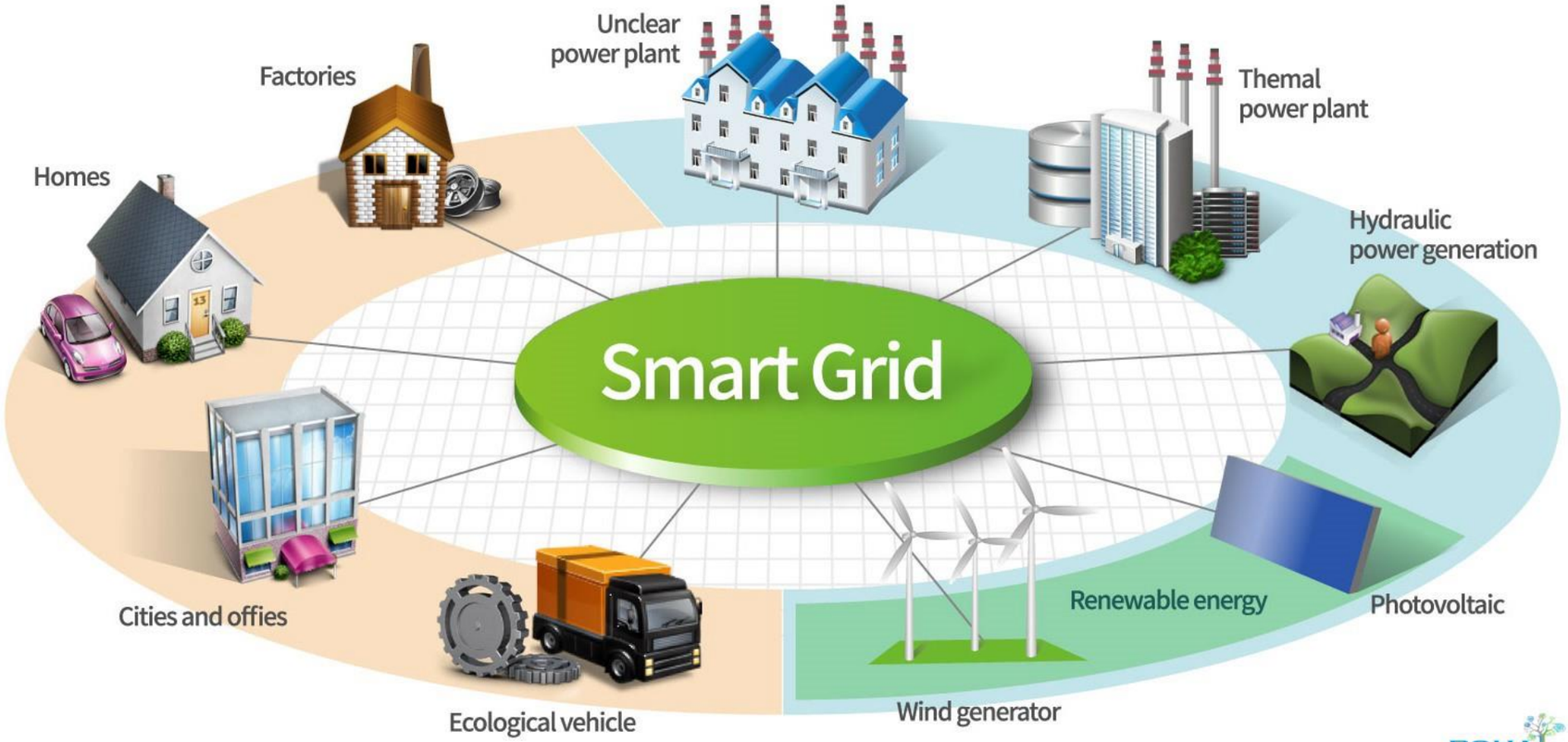
# Background – Power Grid

- SCADA system

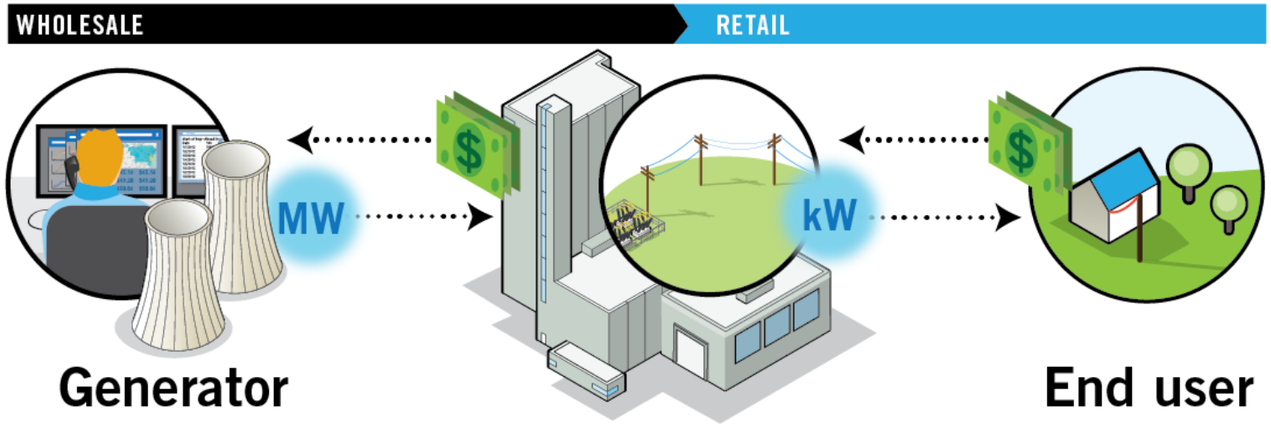
# Background – Power Grid

- Smart grid technologies



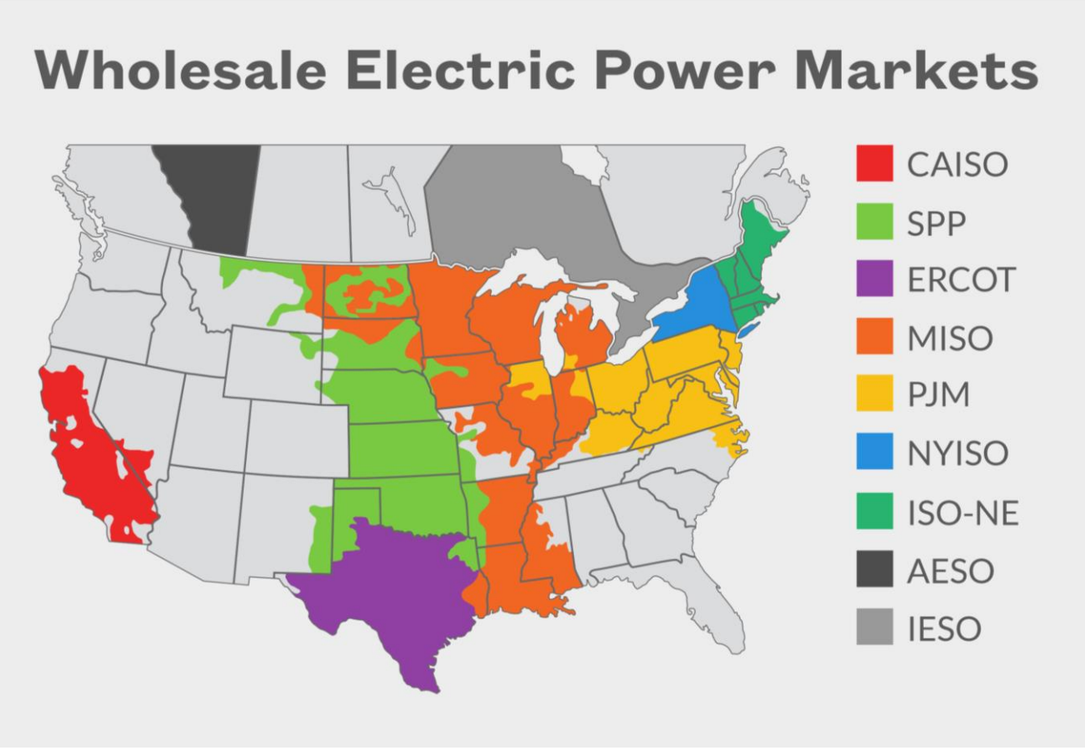
# Background – Electricity Markets

- Restructured system, introduced in late 1990s
- Government-owned to private-owned – competitive environment
- Generation companies, e.g., wind power plants
- Retailers, e.g., utilities
- **167** billion USD in **2018**



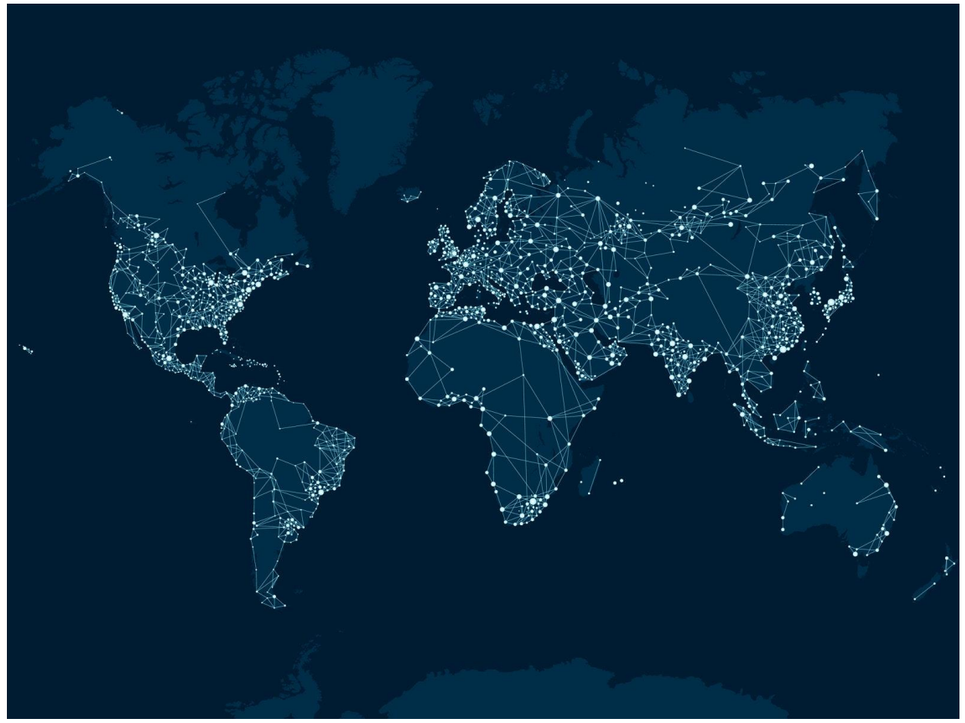
# Background – Electricity Markets

- Different regions around the world
- Each market has two sub-markets: **day-ahead** and **real-time**
- Day-ahead market – load forecasting
- Real-time market – load forecasting errors, unpredictable events



# Background – IoT Botnets

- **Mirai** botnet was discovered in August 2016
- **600,000** compromised devices
- **Indirectly** attack other domains, e.g., Brian Krebs' website
- **DDoS** attacks
- LuaBot, Hajime, BrickerBot



# Attacks on Financial Markets

- Market manipulation?
- Deliberate and malicious **interference** with the **market values** to create an **artificial price** for a tradable entity
- **DDoS** attacks targeting availability
- Operation Digital Tornado - L0ngWave99, April 2012, US markets
- Operation Ababil - Al-Qassam Cyber Fighters, 2012-2013, US markets


# Attacks on Electricity Markets

- Market manipulation in electricity markets
- **FERC** reported **16** potential market manipulation cases in **2018**
- **14** cases were closed with **no action**
- **UK** electricity market attack

EDITORS' PICK | 8,996 views | May 15, 2020, 05:56am EDT

## Cyber Attack On U.K. Electricity Market Confirmed: National Grid Investigates

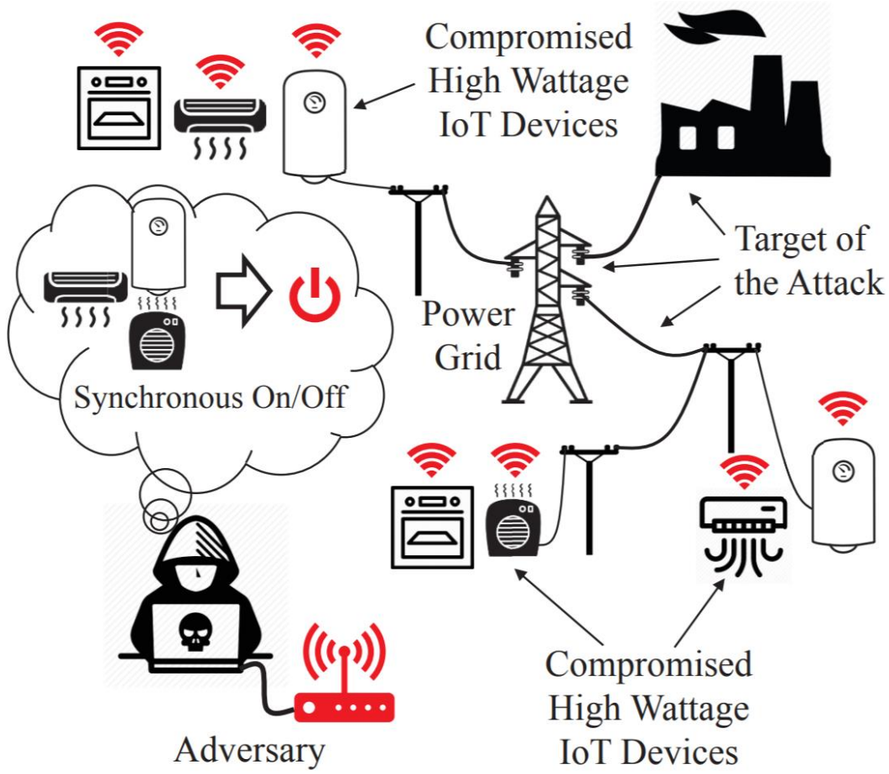
**Davey Winder** Senior Contributor ⓘ

Cybersecurity

*I report and analyse breaking cybersecurity and privacy stories*

# IoT Botnet Attacks on the Power Grid

- Soltan et. al. introduced **BlackIoT** in USENIX Security 2018
- Huang et. al. presented "**not everything is dark and gloomy**" in USENIX Security 2019

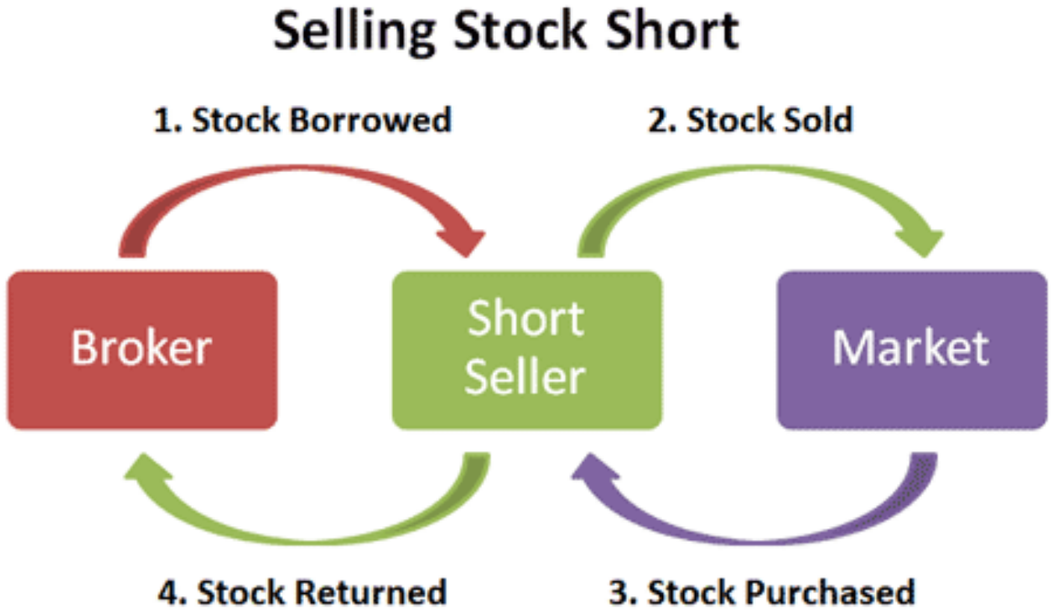


# Threat Model

- Market manipulation in electricity markets? How?!

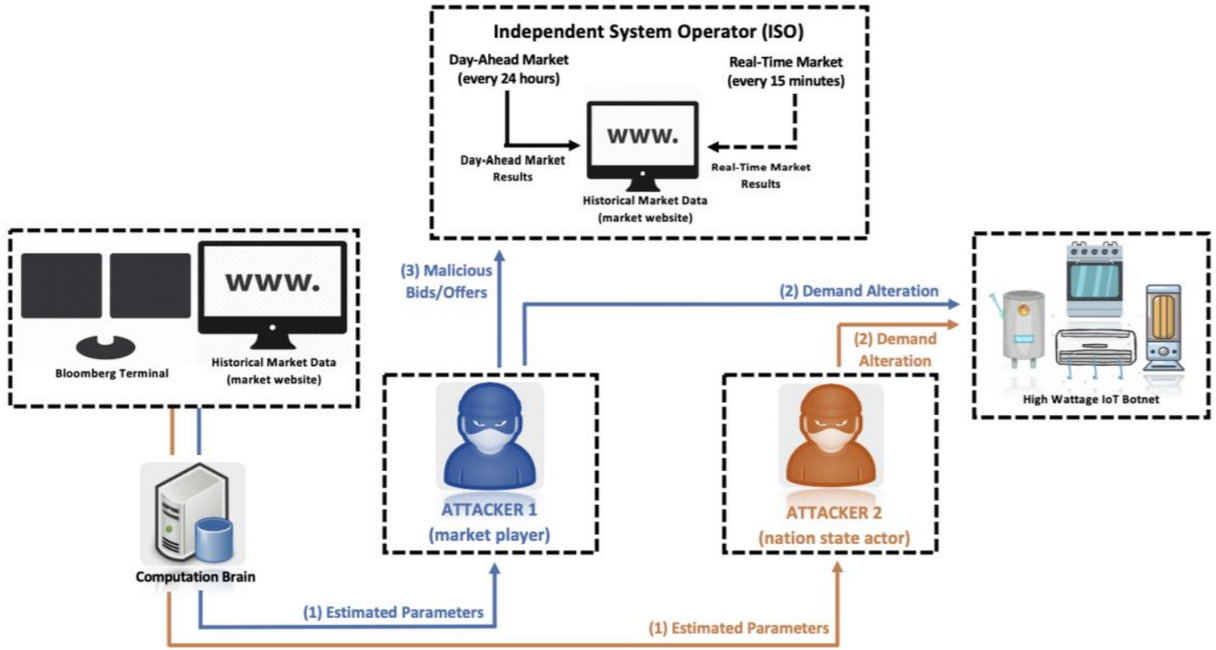
# Threat Model

- Buy a stock in low price, sell after the huge pump
- For example, buy when the price is 2 USD
- Sell when the price is 3 USD
- Sell a stock in high price, buy after the huge dump
- For example, sell when the price is 3 USD
- Buy when the price is 2 USD



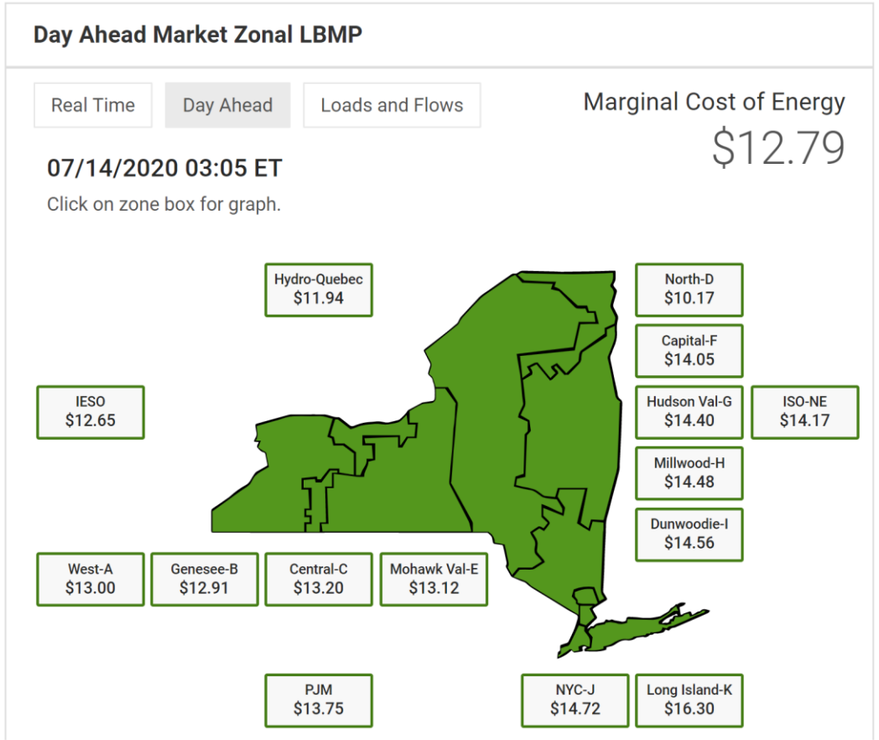
# Threat Model

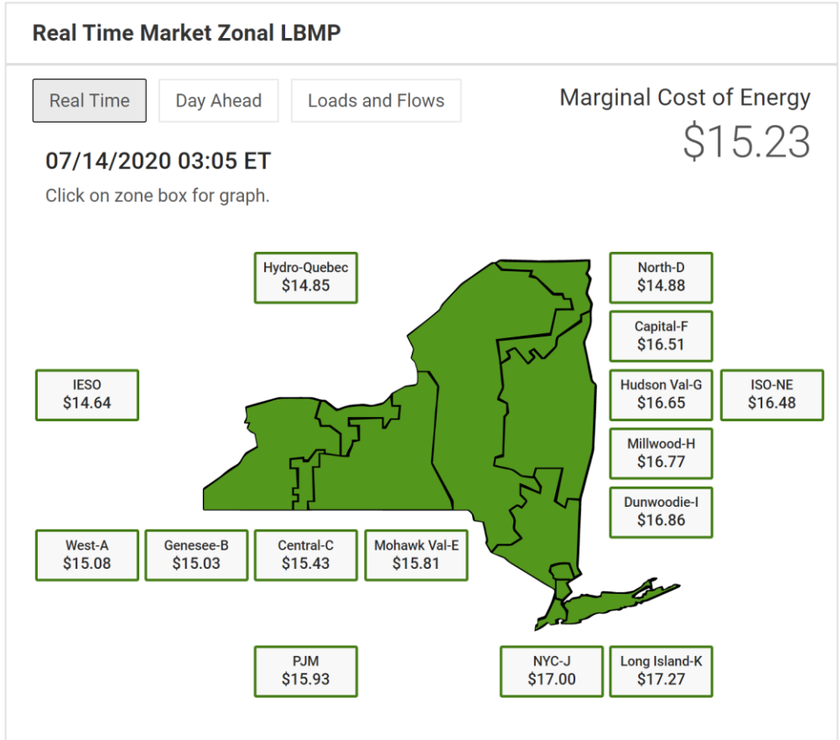
- **System demand change** in real-time affects the electricity market **prices**
- High-wattage IoT botnet
- We can manipulate the profits of different players
- **Attacker type 1:** market player
- **Attacker type 2:** nation state actor



# Threat Model

- The attacker needs market historical and real-time data
  - Price-load sensitivity
  - System real-time demand
  - Day-ahead prices
- Optimize the attack to maximize the gain/damage



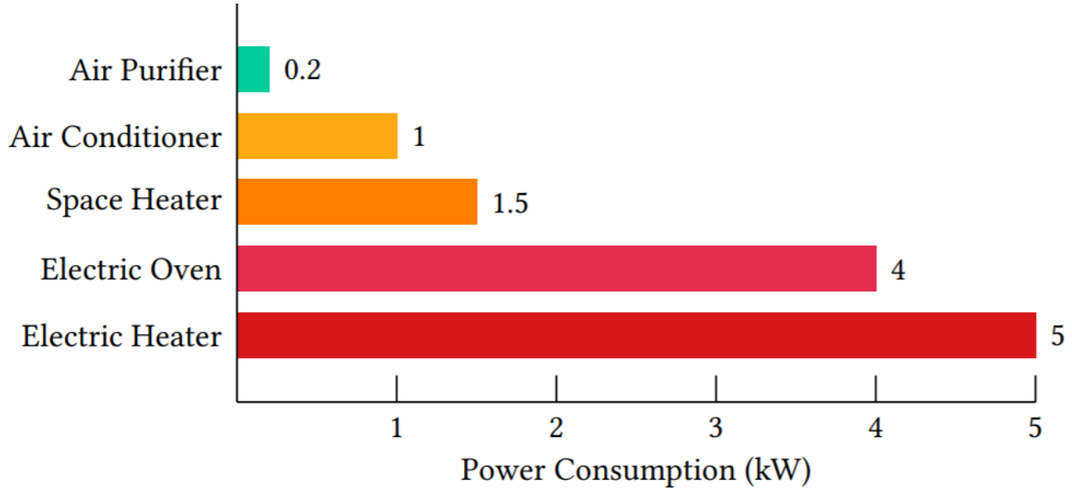



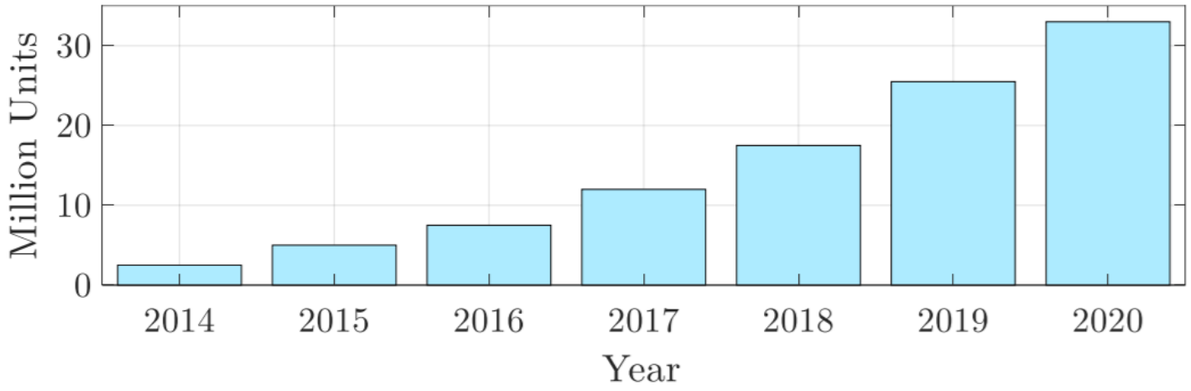
# Threat Model

- **Attacker type 1:** maximize the profit of the market player
- Constraints: technical, market rules, stealth
- **Attacker type 2:** maximize the economic damage on the market
- Constraints: market rules, stealth

# Attack Feasibility

- From the **IoT botnet** perspective
- A successful attack can be done with **50,000 bots**
- Build/Rent with approximately **4000 USD/month**
- Attack gain? **Millions of dollars/day**
- **High-Wattage bots**



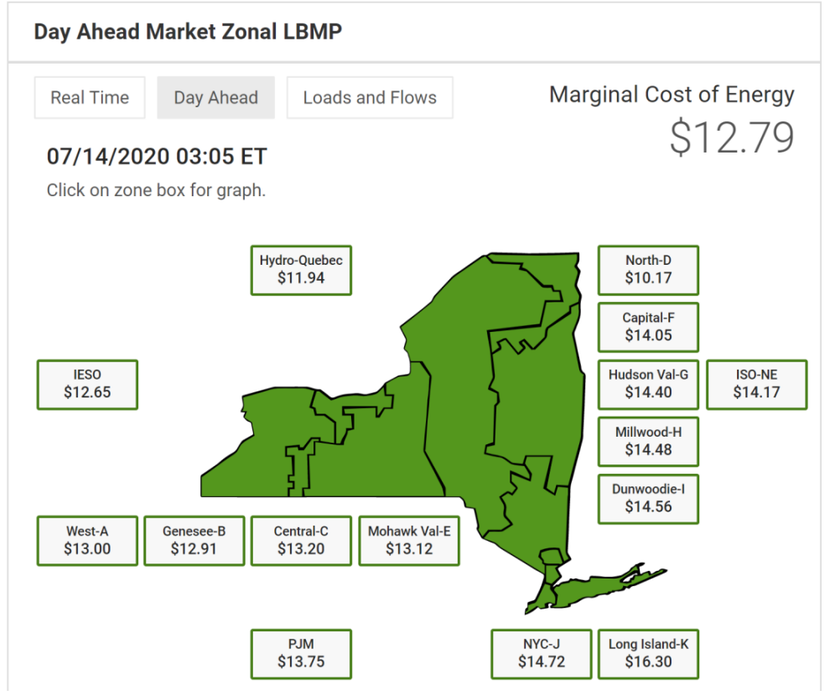
# Attack Feasibility

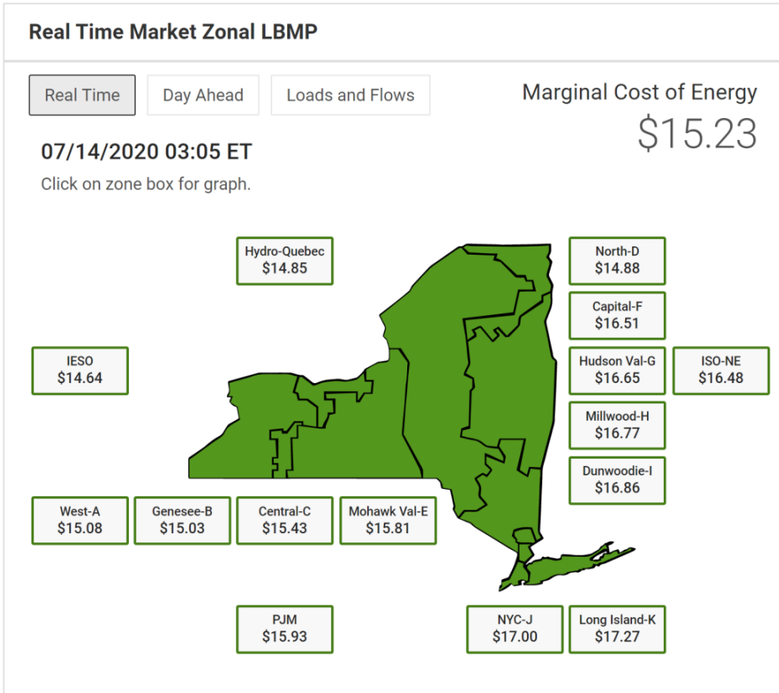
- Available botnet rental services

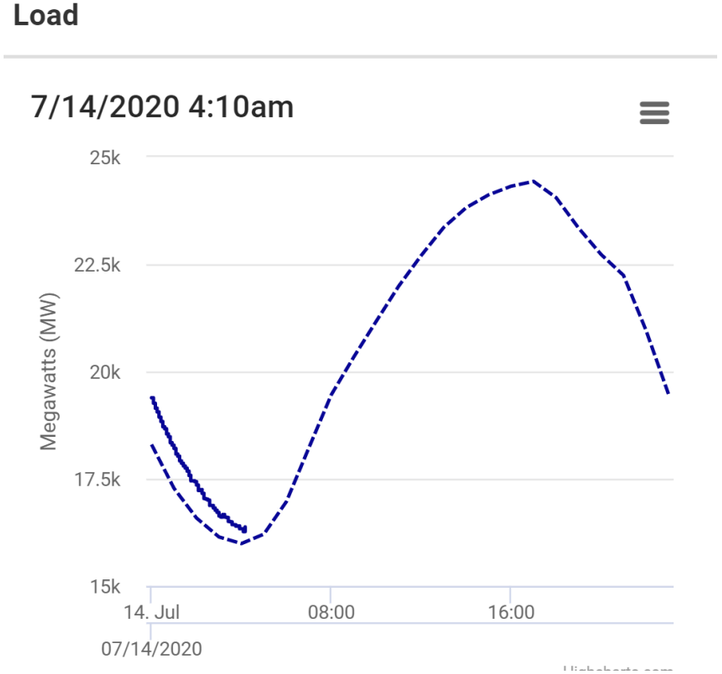
| Name | Botnet Size | Rental Cost | Duration | Bandwidth | Type of Bots |
|---|---|---|---|---|---|
| JenX [34] | - | $20/target | - | 295Gbps | small/office routers |
| Mirai variant [16] | 50k | $3-4000/2 weeks | 1 hour | - | cameras, routers, DVRs, etc. |
| Bushido [43] | 20k | $20-150/month | - | 500Gbps | cameras, routers, DVRs, etc. |
| Reaper [33] | 30k | - | - | - | cameras, routers, DVRs, etc. |
| Satori [35] | 100k | - | - | - | small/office routers |
| Estimate for IoT Botnet Services [9] | - | ~$15/week | - | 300Gbps | - |
| Estimate for DDoS Services [41] | - | $20-45/month | 1 hour | 220Gbps | - |

# Attack Feasibility

- From the **power grid** perspective



# Attack Feasibility

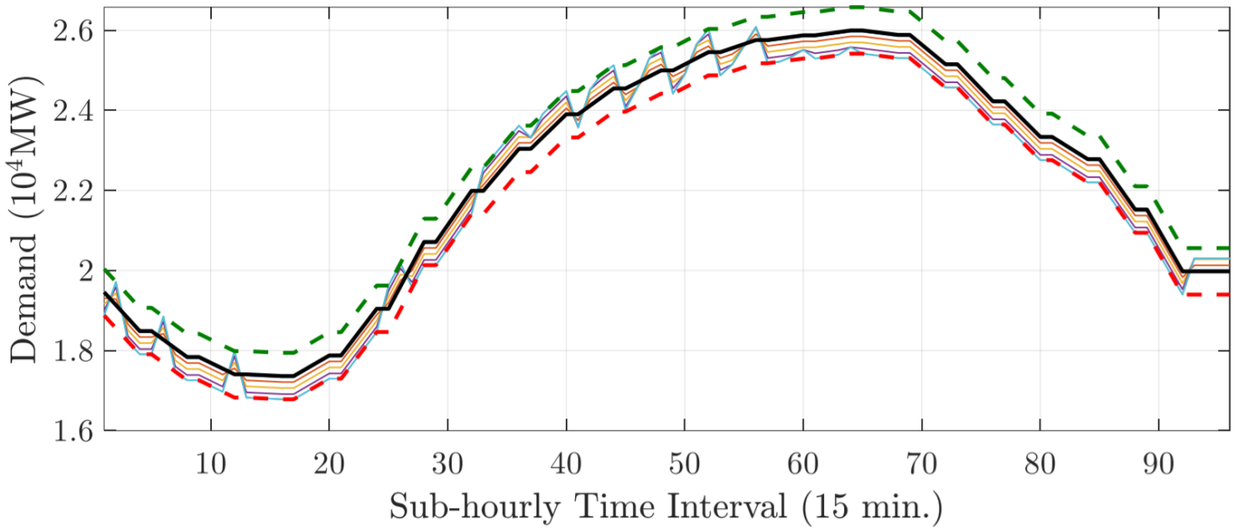
- From the **end user's** perspective
- Average power consumption of Americans is 914 kWh
- Tennessee 1282 kWh, Hawaii 517 kWh
- Each bot 3 kW
- 100 days per year (8 days per month)
- 3 hours on average
- **7%** increase in the billing statement (most severe case!)

# Stealth Strategies

- To guarantee the **repeatability**, the attack should be **stealthy**
- **Stealth** increases the **attack gain** in general
- **Increased attack gain** adds to the motivation of the attackers
- **Stealth** adds to the motivation of the attackers to avoid **law-related repercussions**

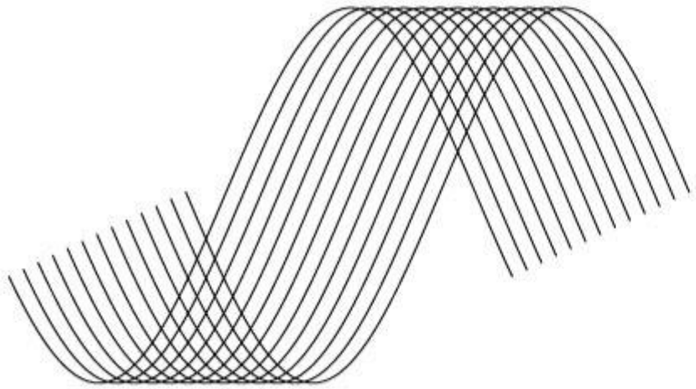
# Stealth Strategies

- Smooth Load Profile
- Change the demand severely? **Detected!**
- Typical **load forecasting error**



# Stealth Strategies

- Frequency of attack
- Launch the attack **every day**? Too much **risk**!
- **100 days/year** is **reasonable** (8 days/month)
- For lower risks, the attacker can try 50 days/year (4 days/month)



*frequency*

# Stealth Strategies

- Implementing **sub-optimal** attack scenarios
- Choosing a sub-optimal attack vector
- Makes it hard for the **market analyzers** to detect the attack
- Might find other **innocent players guilty**

# Stealth Strategies

- Deliberately target other players
- The attacker might intentionally target his **competitors**
- To **damage** certain companies/players
- **Lift the suspicion** from himself

# Stealth Strategies

- **Smart** botnet use in every home
- E.g., the EV has been proven to have great potential!

| Smart IoT Device | Energy Consumption (W) | Peak Use Time | Avg Use Length | Time to Attack |
|---|---|---|---|---|
| Water Heater [47] | 5000 | Morning | 3h/day | Early Morning |
| AC [74] | 1000 | All-day | 9h/day | Anytime |
| f Garage Opener [39] | 1100 | All-day | 3min/day | Midday |
| Fridge [61] | 900 | All-day | 24h/day | Midday |
| Heater [27] | 1500 | Evening | 3h/day | Anytime |
| EV charger [56] | 12000 | Evening | 8h/day | Early Morning |
| Oven and Stove [48] | 4000 | Evening | 1h/day | Early Morning |
| Washer [30] | 1200 | Sporadic | 2h/wk | Early Morning |
| Dryer [30] | 1800 | Sporadic | 2h/wk | Early Morning |
| Dishwasher [83] | 852 | Sporadic | 120min/day | Early Morning |
| Treadmill [11] | 735 | Sporadic | 90min/wk | Early Morning |

E&E NEWS

SEARCH: enter keyword go!

<< Back to E&E News index page.

CYBERSECURITY

## 'Major vulnerability': EV hacks could threaten power grid

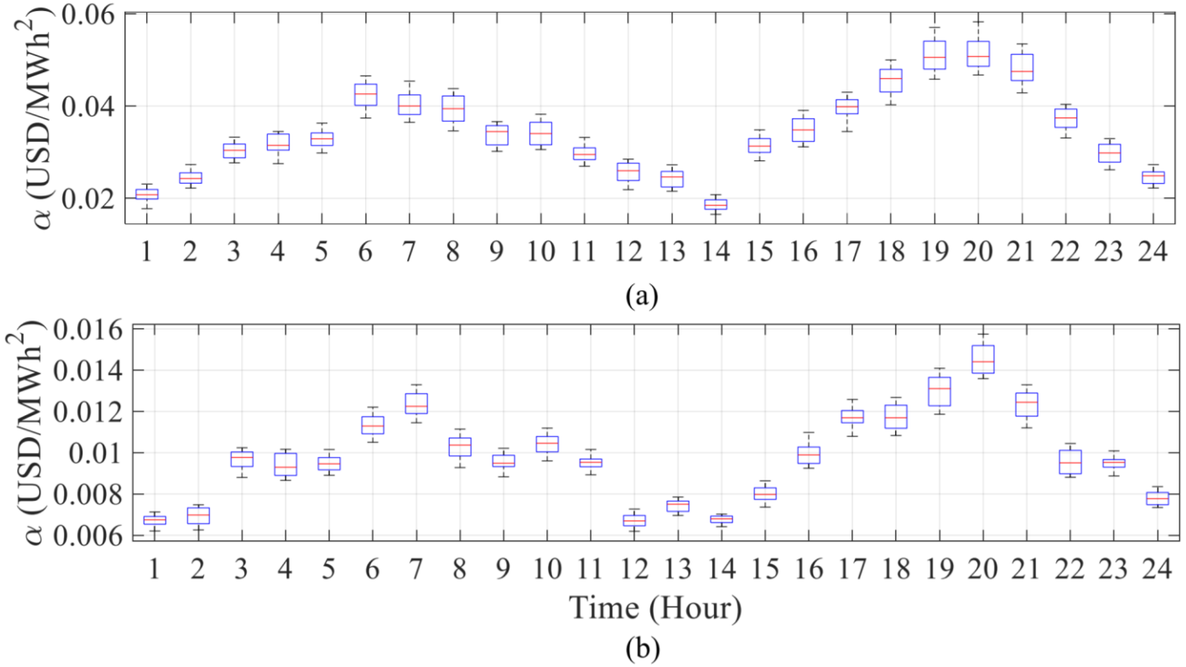
Christian Vasquez, E&E News reporter • Published: Wednesday, June 17, 2020

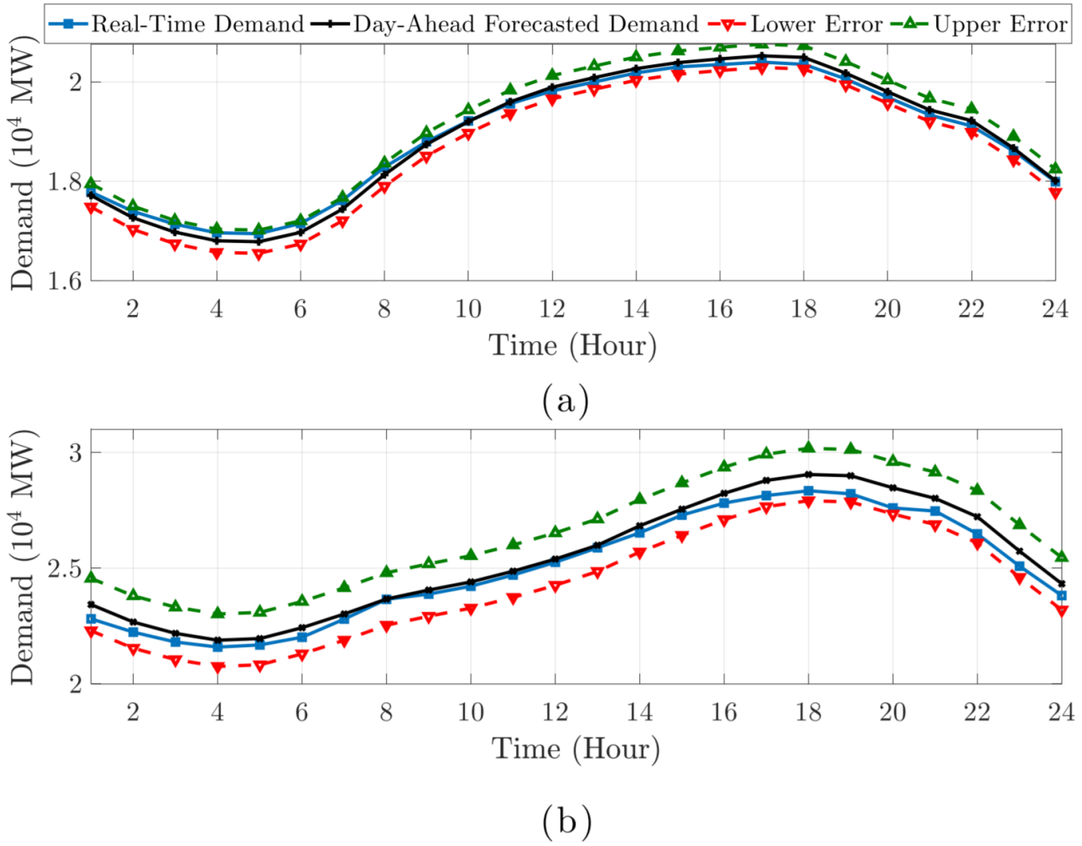
# Numerical Results

- For evaluation purposes, **real-world implementation** is not possible!
- We used the **real-world data analysis** for the two biggest electricity markets in the US, **New York and California markets**
- One-year data were used, May 2018 – May 2019


# Numerical Results

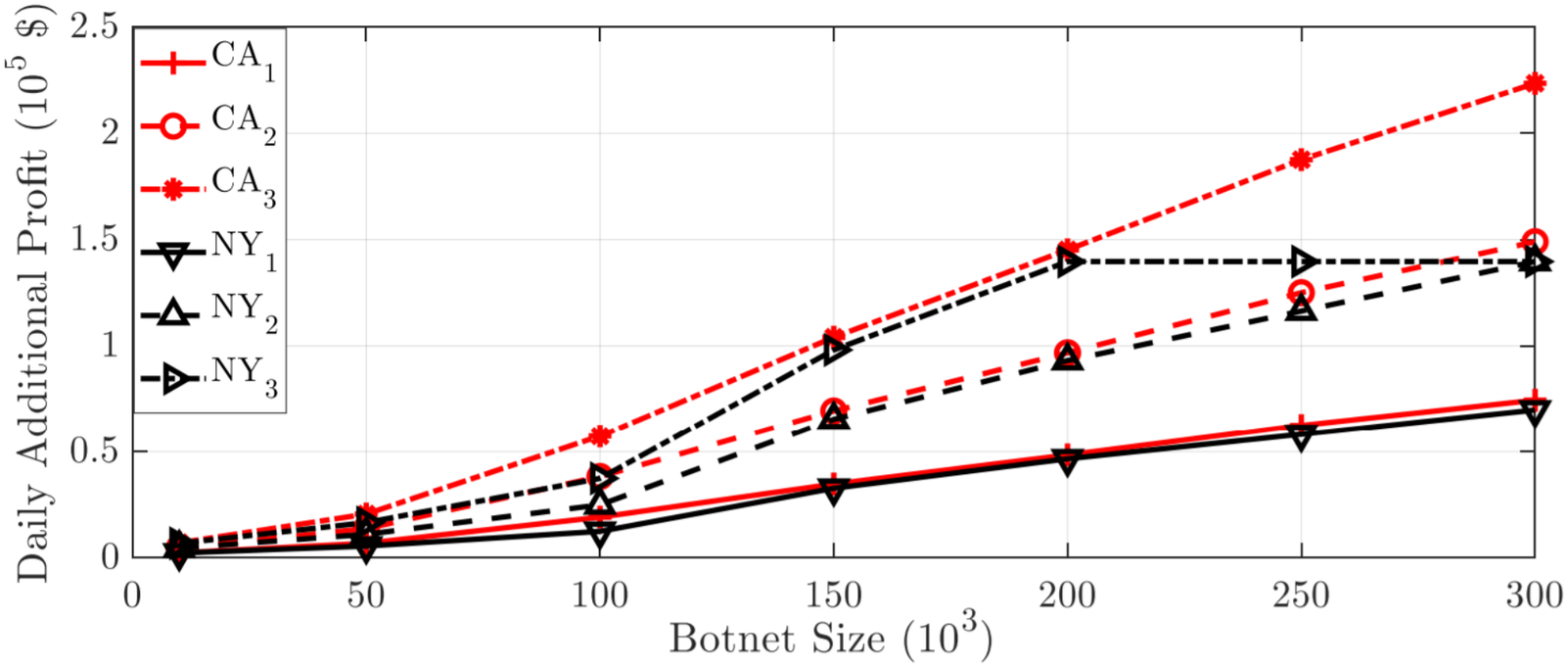
- Estimating the **key parameters** based on historical data



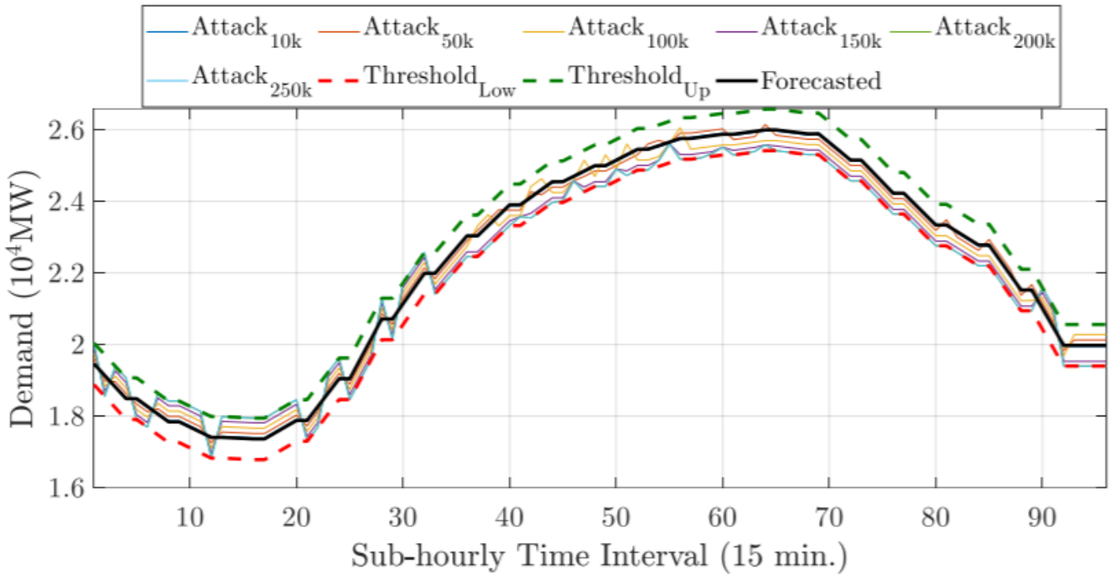
# Numerical Results

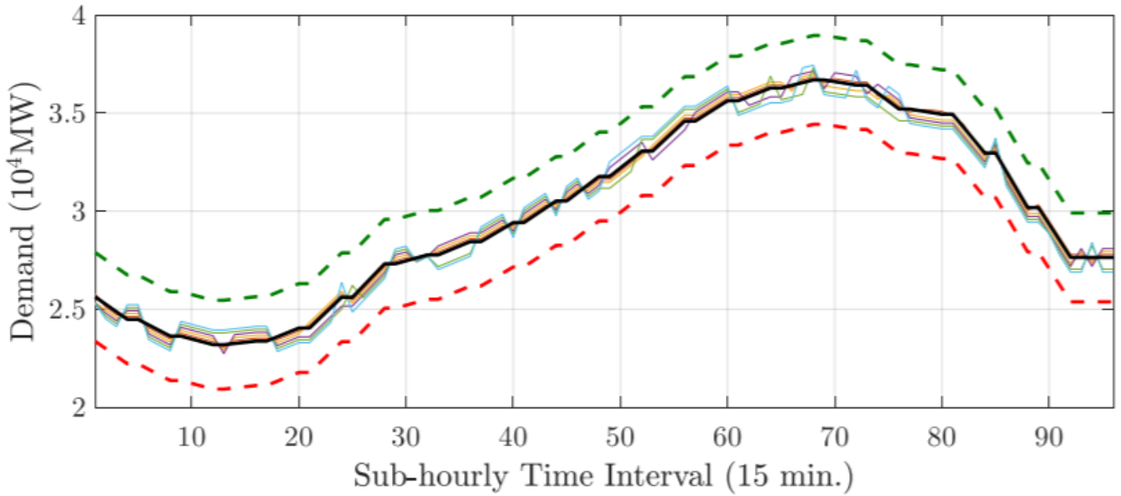
- Attacker type 1– attacker is a market player
- A typical power plant owner with 2000 MW capacity



# Numerical Results

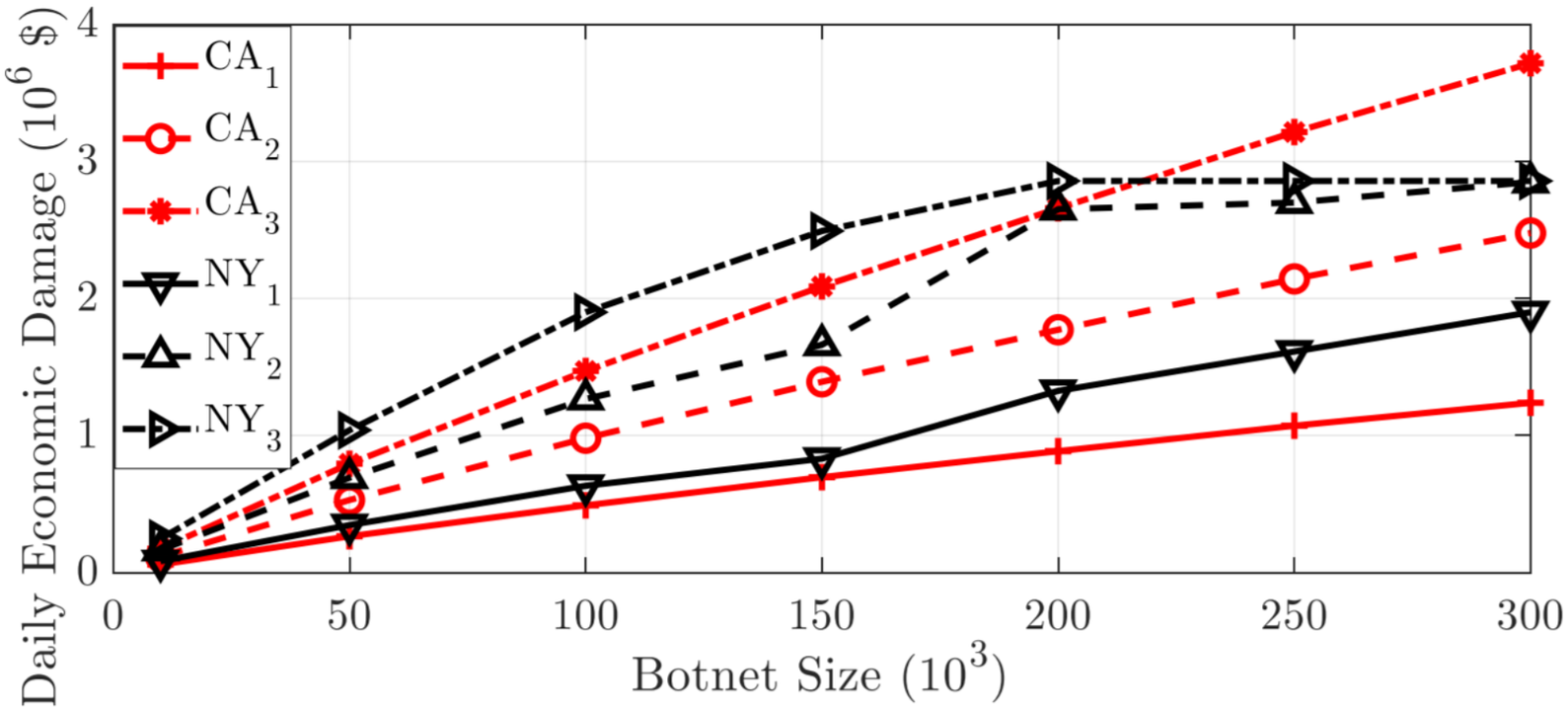
- Attacker type 1– attacker is a market player



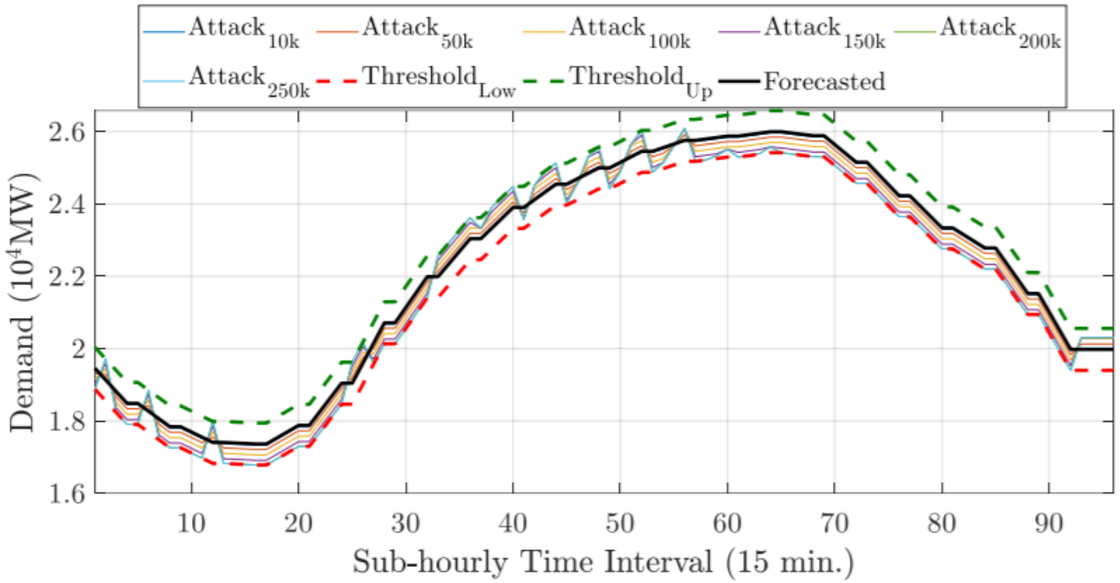
# Numerical Results

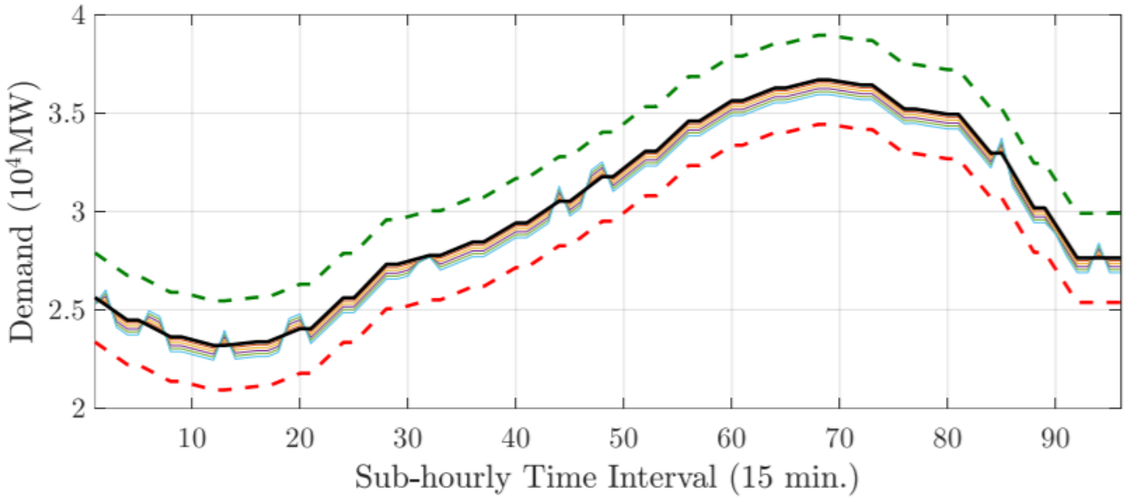
- Attacker type 2 – nation state actor
- Targeting the generation side companies



# Numerical Results

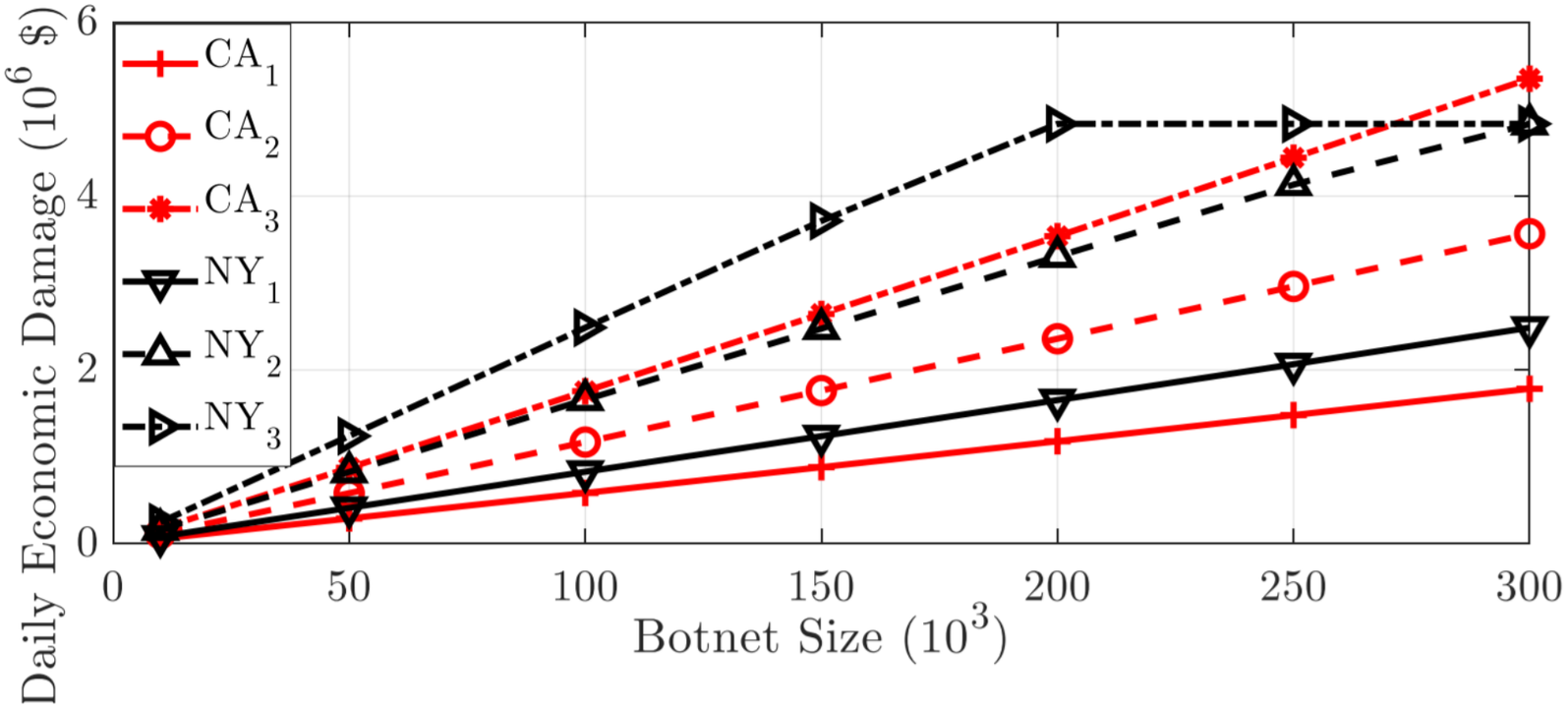
- Attacker type 2 – nation state actor



# Numerical Results

- Attacker type 2 – nation state actor
- Targeting the demand side companies (retailers)



# Countermeasures

- **Real-Time** IoT Monitoring Database
- Small fraction of the **high-wattage IoT devices** can be registered and monitored in an online database

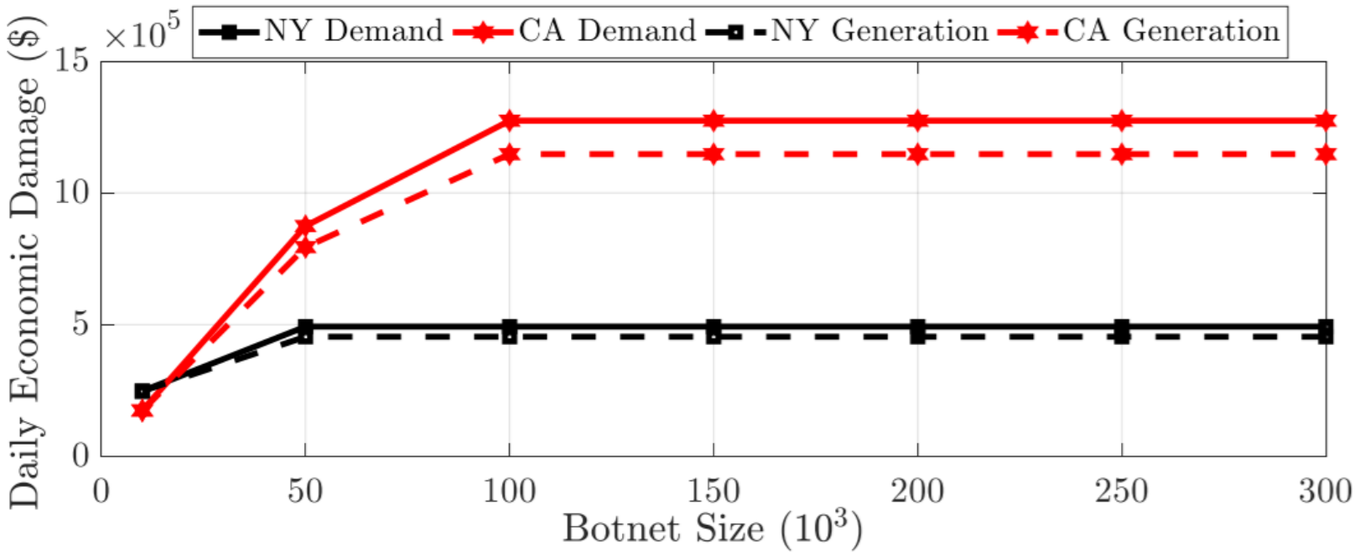
Honeywell

Nest

Schneider Electric

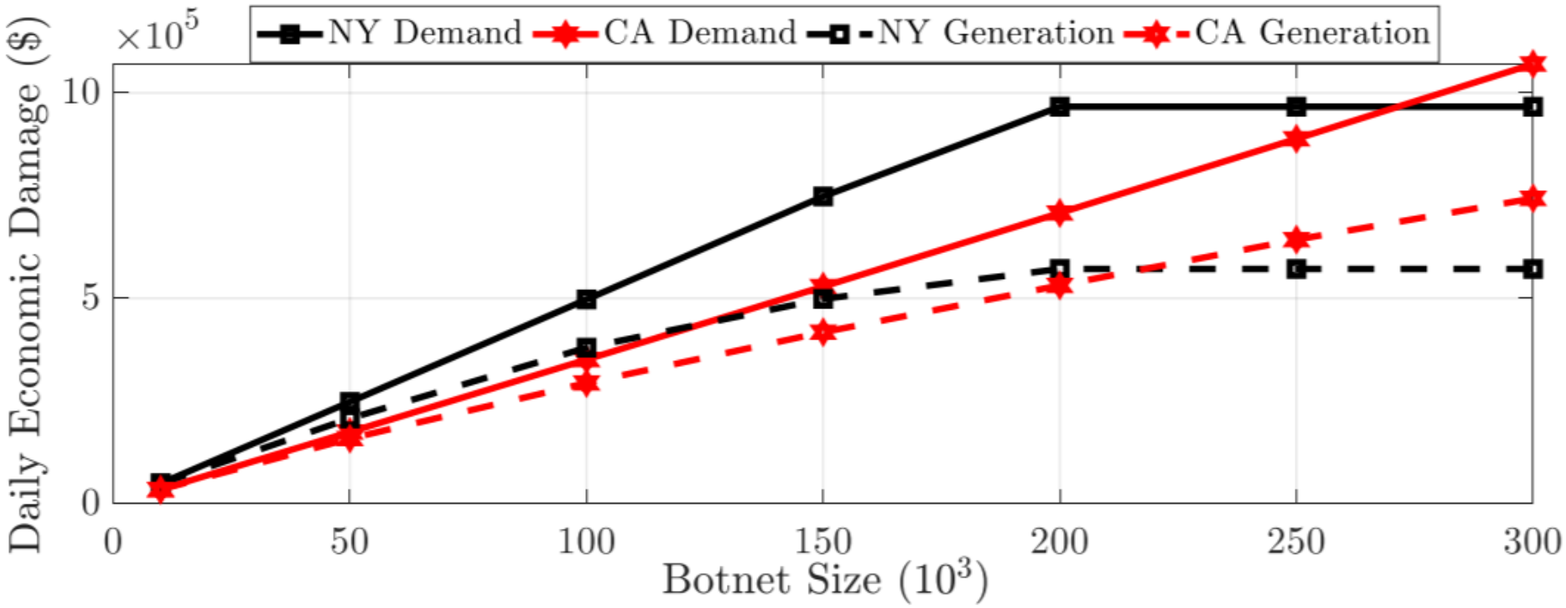
# Countermeasures

- **Revisited** market data sharing
- **Data privacy plans** might be effective for nation state attackers
- For the market players, preprocessed delayed data should be shared



# Countermeasures

- Limit the **price sensitivity** in real-time market



# Conclusions and Possible Directions

- IoT botnet-based attack on the electricity market
- Its effect was analyzed on two sample big electricity markets in the US, **California and New York markets**
- **24 million USD** further yearly profit can be obtained by a malicious market player
- **350 million USD** economic damage can be done by the nation state actor
- A set of practical countermeasures were introduced, the attack gain can be reduced by **80%**
- We hope to raise the attention of the **market operators**
- Further **research/analysis on** the effective **countermeasures**

# Thank You!

# Questions?!