PRINCETON
UNIVERSITY

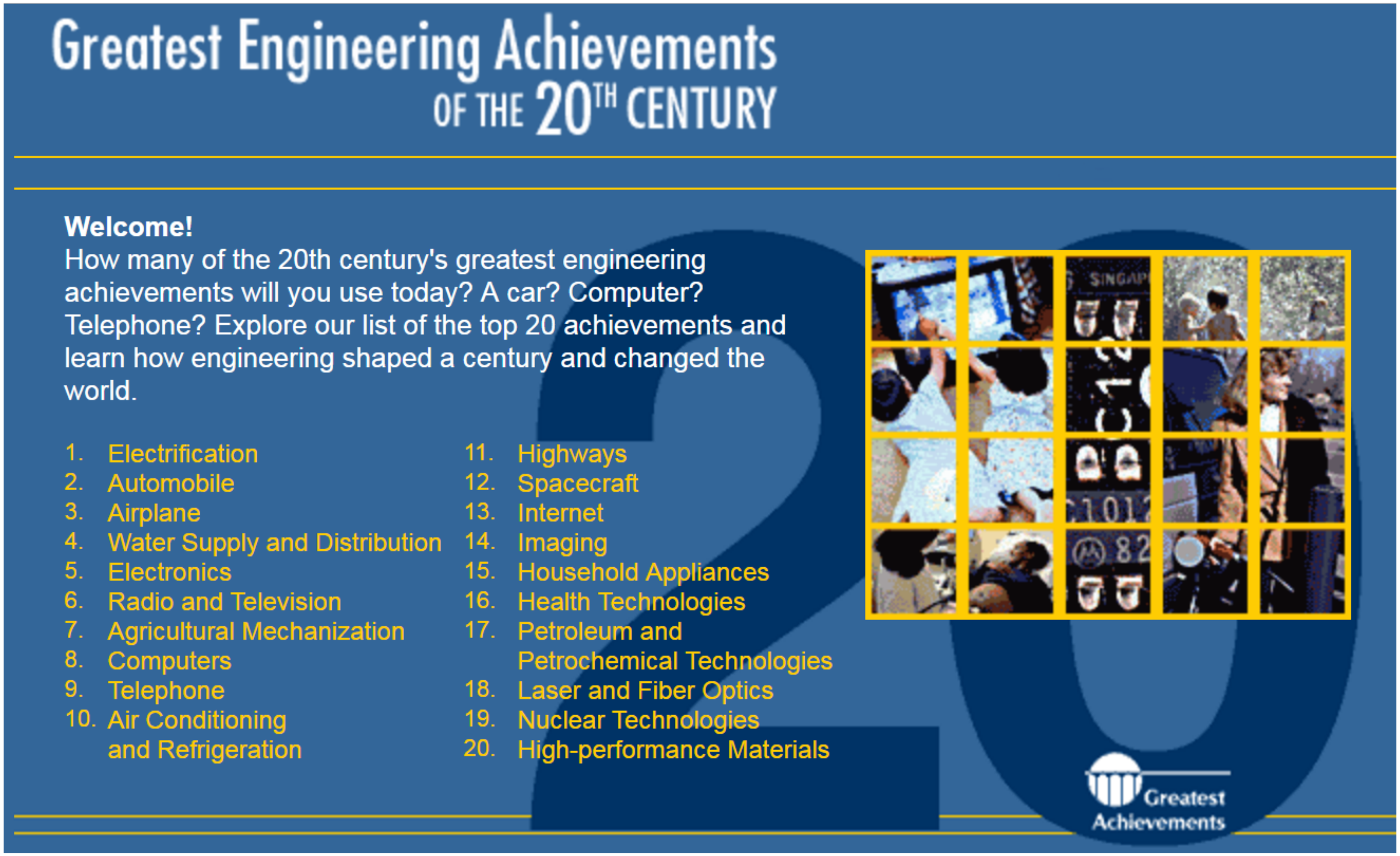
BlackIoT: IoT Botnet of High Wattage Devices Can Disrupt the Power Grid

Saleh Soltan, Prateek Mittal, H. Vincent Poor
Department of Electrical Engineering, Princeton University

USENIX Security'18
August 2018

Electric Power Systems

- One of the most essential infrastructure systems



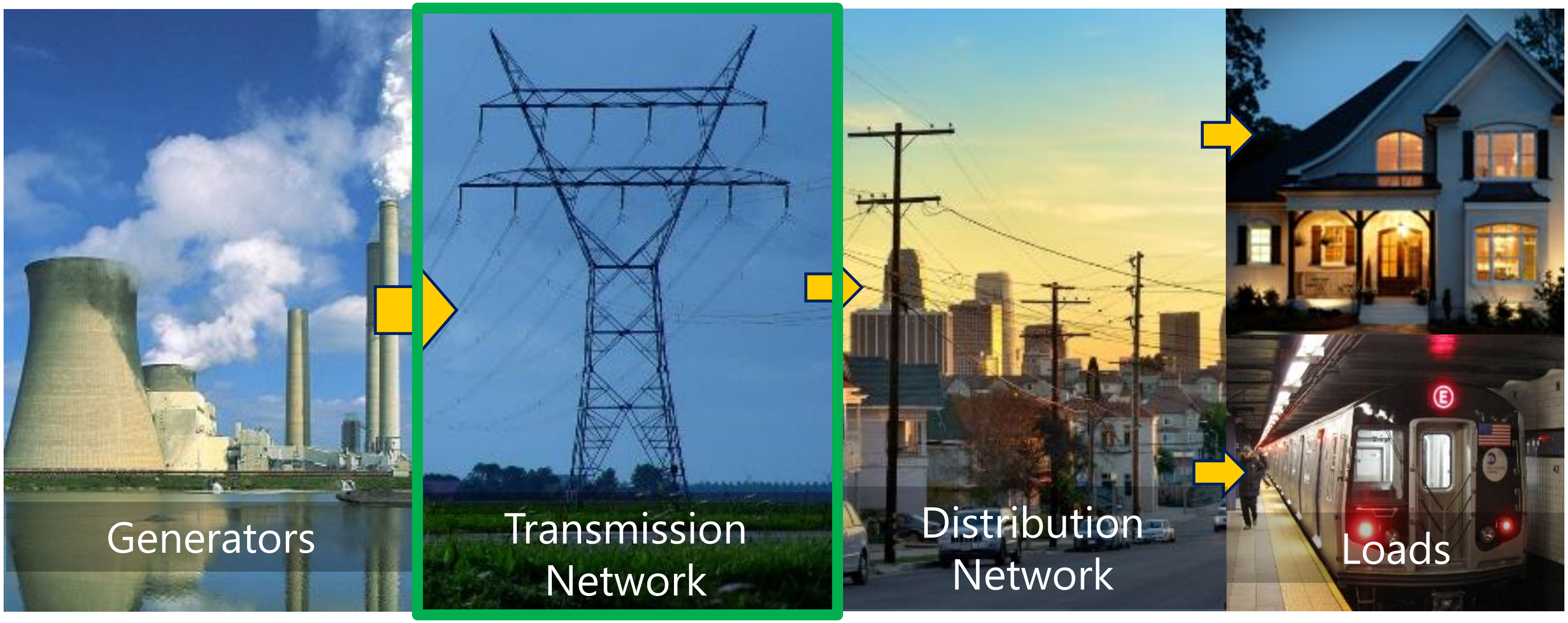
Greatest Engineering Achievements OF THE 20TH CENTURY

Welcome!
How many of the 20th century's greatest engineering achievements will you use today? A car? Computer? Telephone? Explore our list of the top 20 achievements and learn how engineering shaped a century and changed the world.

1. Electrification
2. Automobile
3. Airplane
4. Water Supply and Distribution
5. Electronics
6. Radio and Television
7. Agricultural Mechanization
8. Computers
9. Telephone
10. Air Conditioning and Refrigeration
11. Highways
12. Spacecraft
13. Internet
14. Imaging
15. Household Appliances
16. Health Technologies
17. Petroleum and Petrochemical Technologies
18. Laser and Fiber Optics
19. Nuclear Technologies
20. High-performance Materials

Source: http://www.greatachievements.org/

Major Components of Power Systems



Generators

Transmission Network

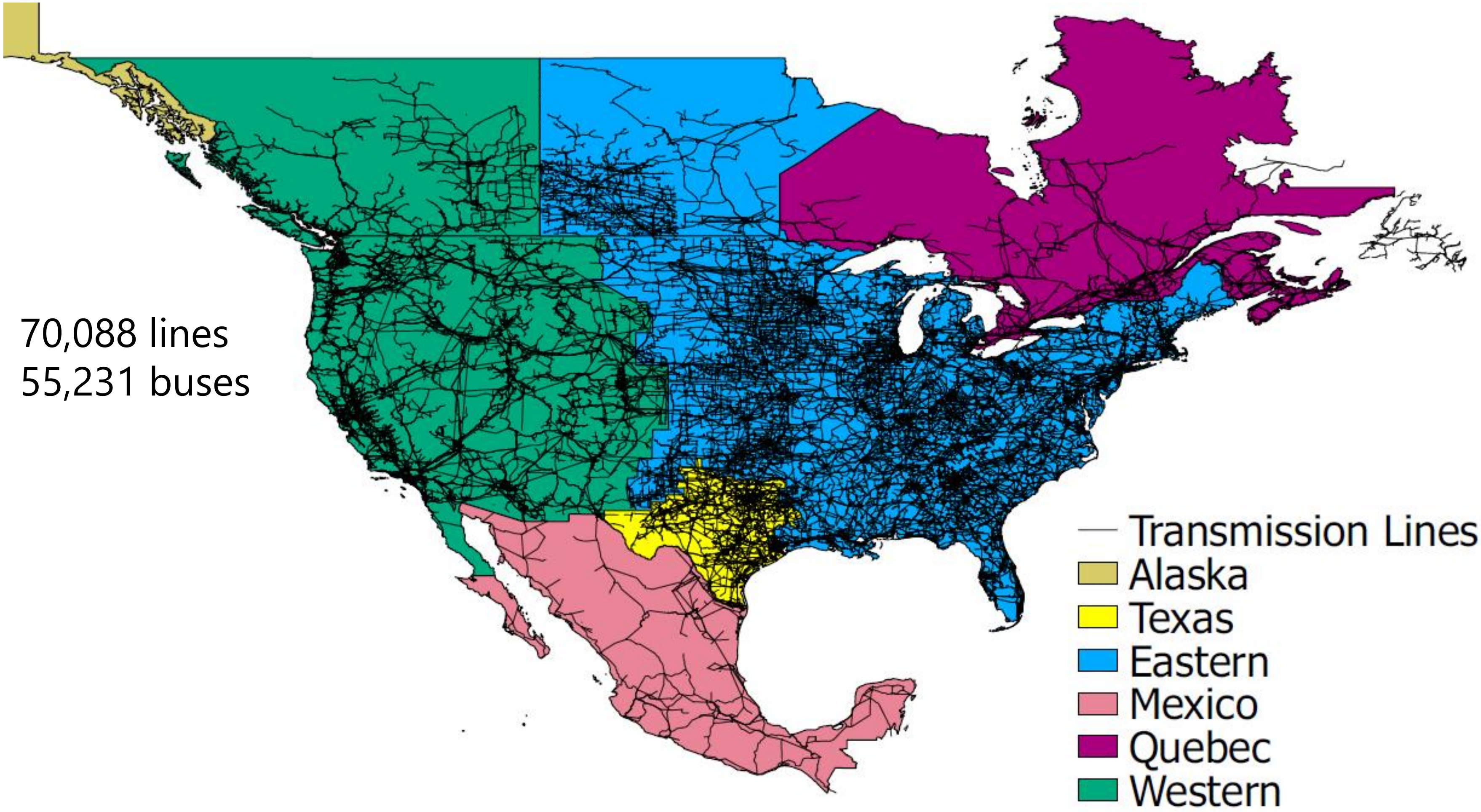
Distribution Network

Loads

765 kV-110 kV

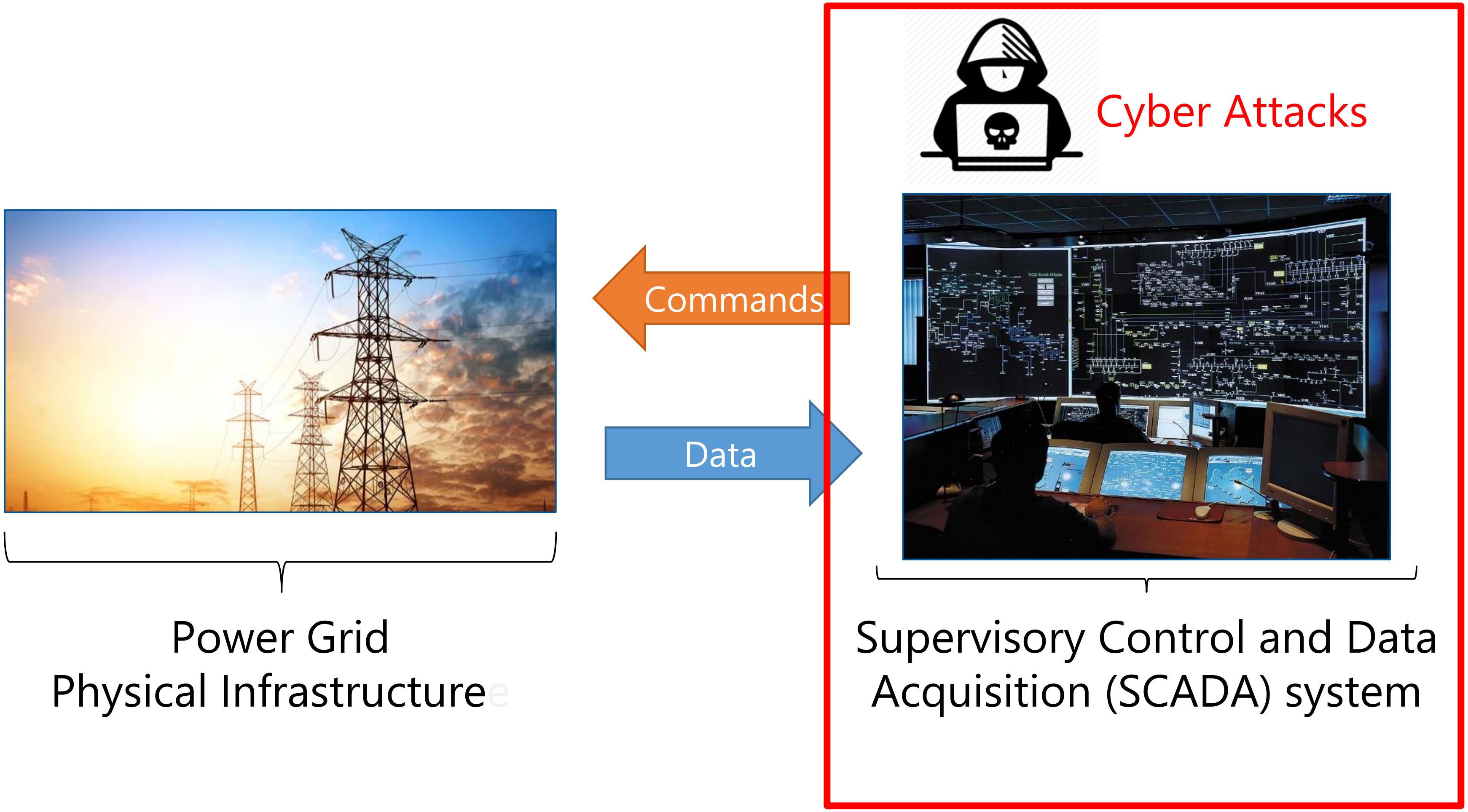
34.5 kV-110 V

North America Transmission Network



70,088 lines
55,231 buses

Power Grid’s SCADA System



Cyber Attacks

Commands

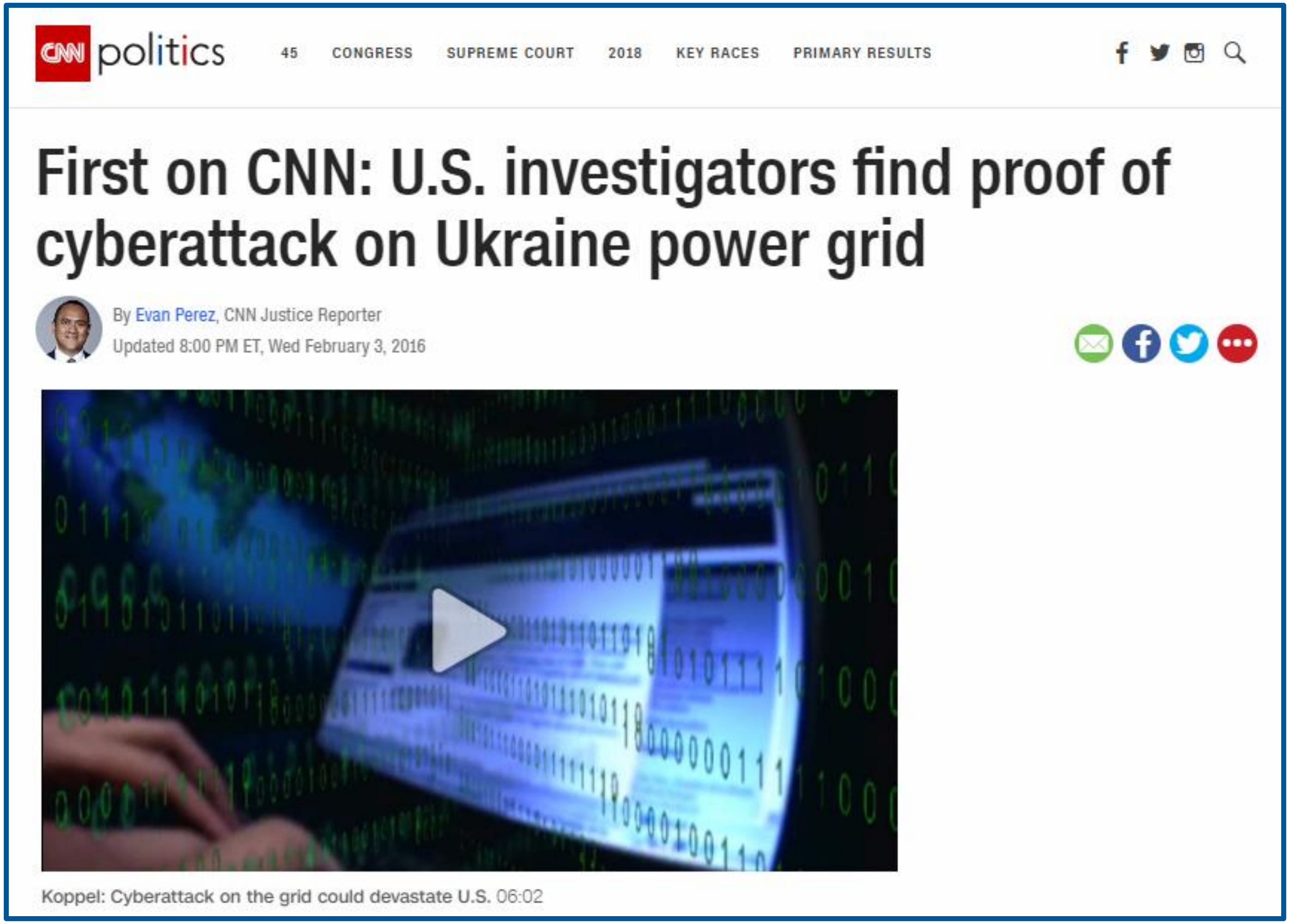
Data

Power Grid
Physical Infrastructuree

Supervisory Control and Data Acquisition (SCADA) system

Cyber Attack on Ukraine Grid's SCADA

- Unplugged 225,000 people from the Ukrainian electricity grid in December 2015



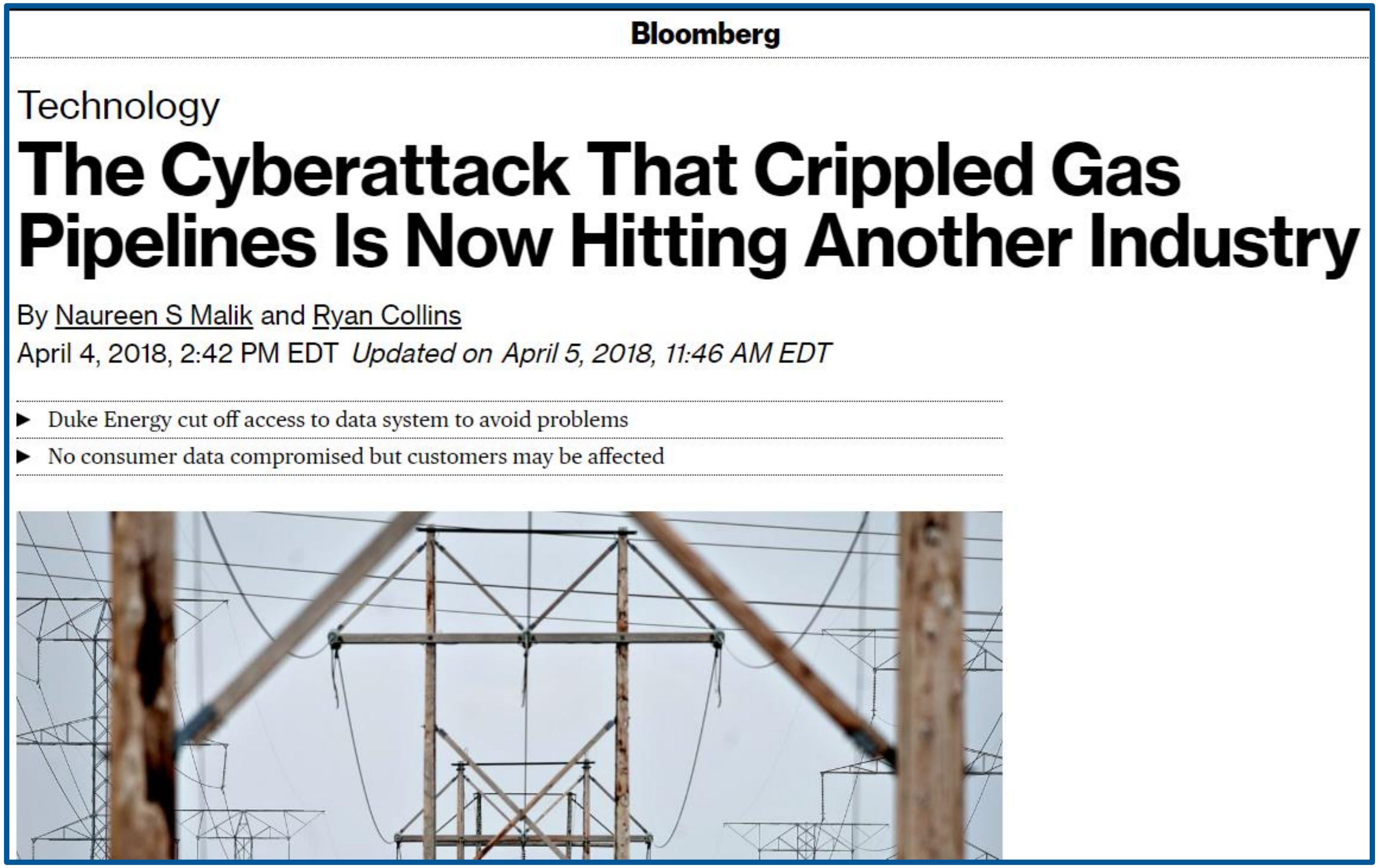
First on CNN: U.S. investigators find proof of cyberattack on Ukraine power grid

By Evan Perez, CNN Justice Reporter
Updated 8:00 PM ET, Wed February 3, 2016

Koppel: Cyberattack on the grid could devastate U.S. 06:02

Cyber Attacks on U.S. Grid SCADA

- Smaller scale attacks on reginal U.S. grids have been investigated in a recent report, April 2018
- *“Hackers are developing a penchant for attacks on energy infrastructure because of the impact the sector has on people’s lives.*"



Bloomberg

Technology

The Cyberattack That Crippled Gas Pipelines Is Now Hitting Another Industry

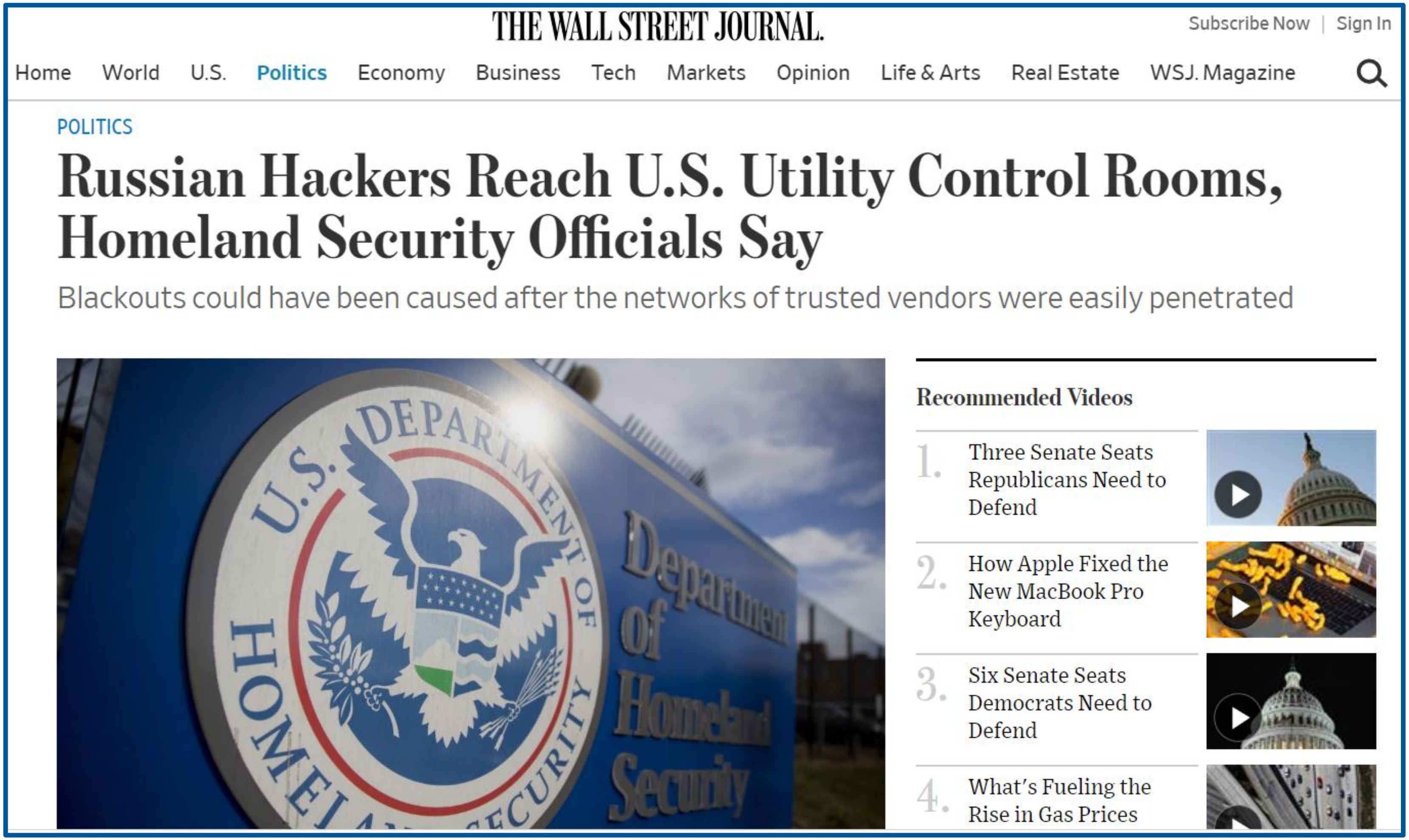
By Naureen S Malik and Ryan Collins

April 4, 2018, 2:42 PM EDT *Updated on April 5, 2018, 11:46 AM EDT*

- ▸ Duke Energy cut off access to data system to avoid problems
- ▸ No consumer data compromised but customers may be affected

U.S. Grid’s SCADA Breaches

- “They got to the point where they could have thrown switches” and disrupted power flows, July 2018



THE WALL STREET JOURNAL.

Subscribe Now | Sign In

POLITICS

Russian Hackers Reach U.S. Utility Control Rooms, Homeland Security Officials Say

Blackouts could have been caused after the networks of trusted vendors were easily penetrated

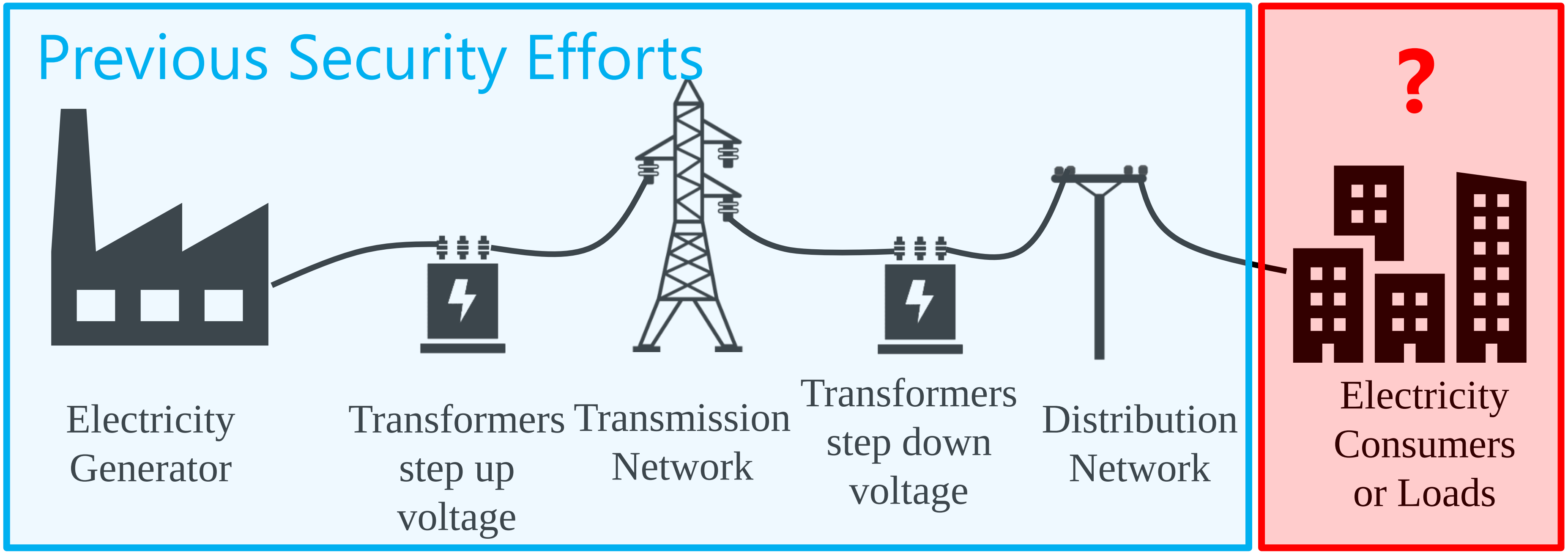
U.S. DEPARTMENT OF HOMELAND SECURITY
Department of Homeland Security

Recommended Videos

1. Three Senate Seats Republicans Need to Defend
2. How Apple Fixed the New MacBook Pro Keyboard
3. Six Senate Seats Democrats Need to Defend
4. What’s Fueling the Rise in Gas Prices

Grid Cyber Security Efforts

- ❑ Previously: the power demand can be predicted reliably on an hourly and daily basis
- ❑ Now: with growth in the number of Wi-Fi enabled high-wattage devices such as air *conditioners and heaters,* is this still a safe assumption?



Previous Security Efforts
Electricity Generator
Transformers step up voltage
Transmission Network
Transformers step down voltage
Distribution Network
?
Electricity Consumers or Loads

IoT Botnet of High-Wattage Devices

- Smart appliances' power usage

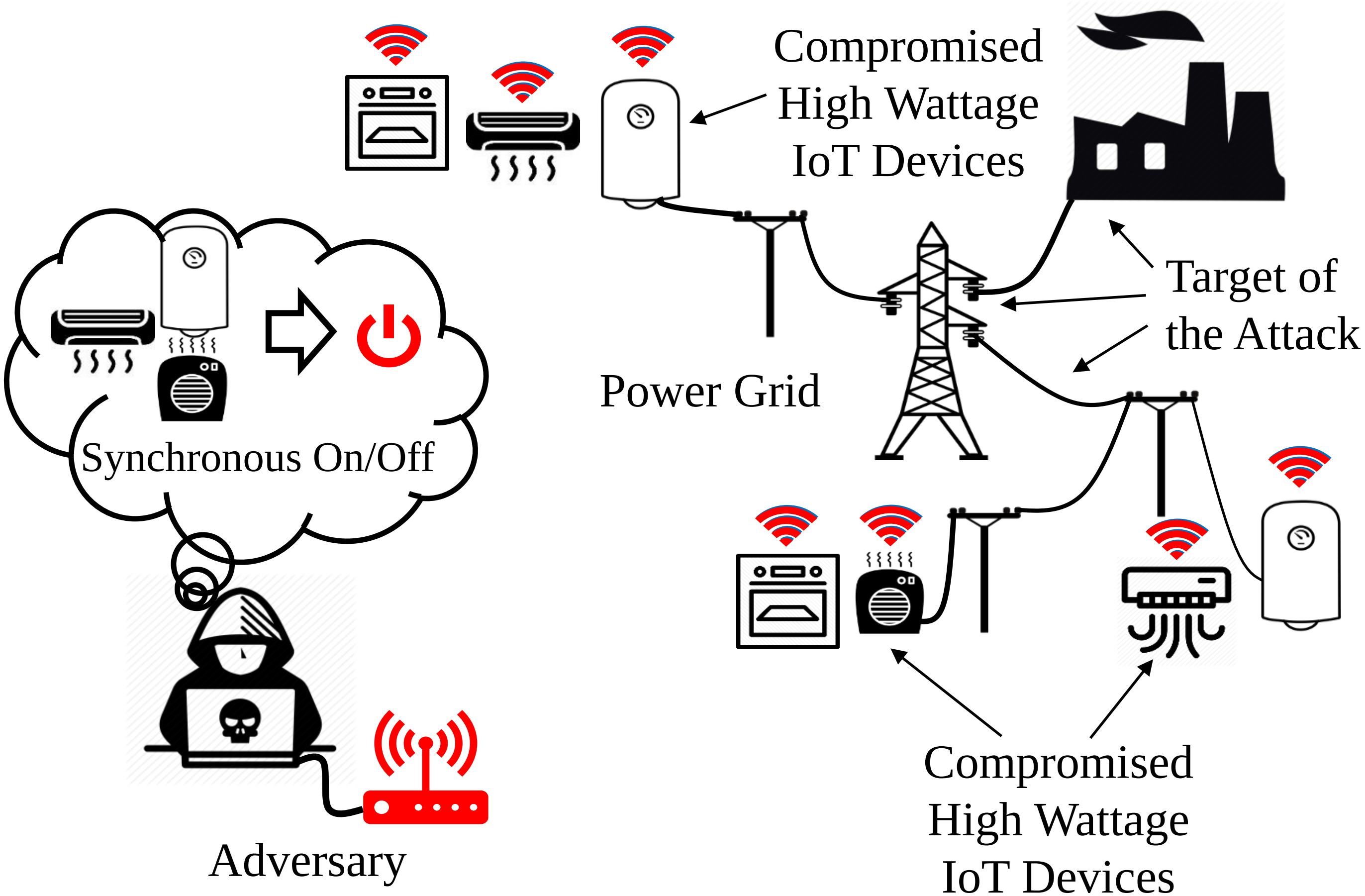
Appliance	Power Usage (W)
Air conditioner	1,000
Space heater	1,500
Air purifier	200
Electric water heater	5,000
Electric oven	4,000

- The *Mirai* botnet → 600,000 bots
- A Mirai sized botnet of water heaters can change the demand instantly in an area by 3000MW!

Similar to having access to the largest currently deployed nuclear power plant!

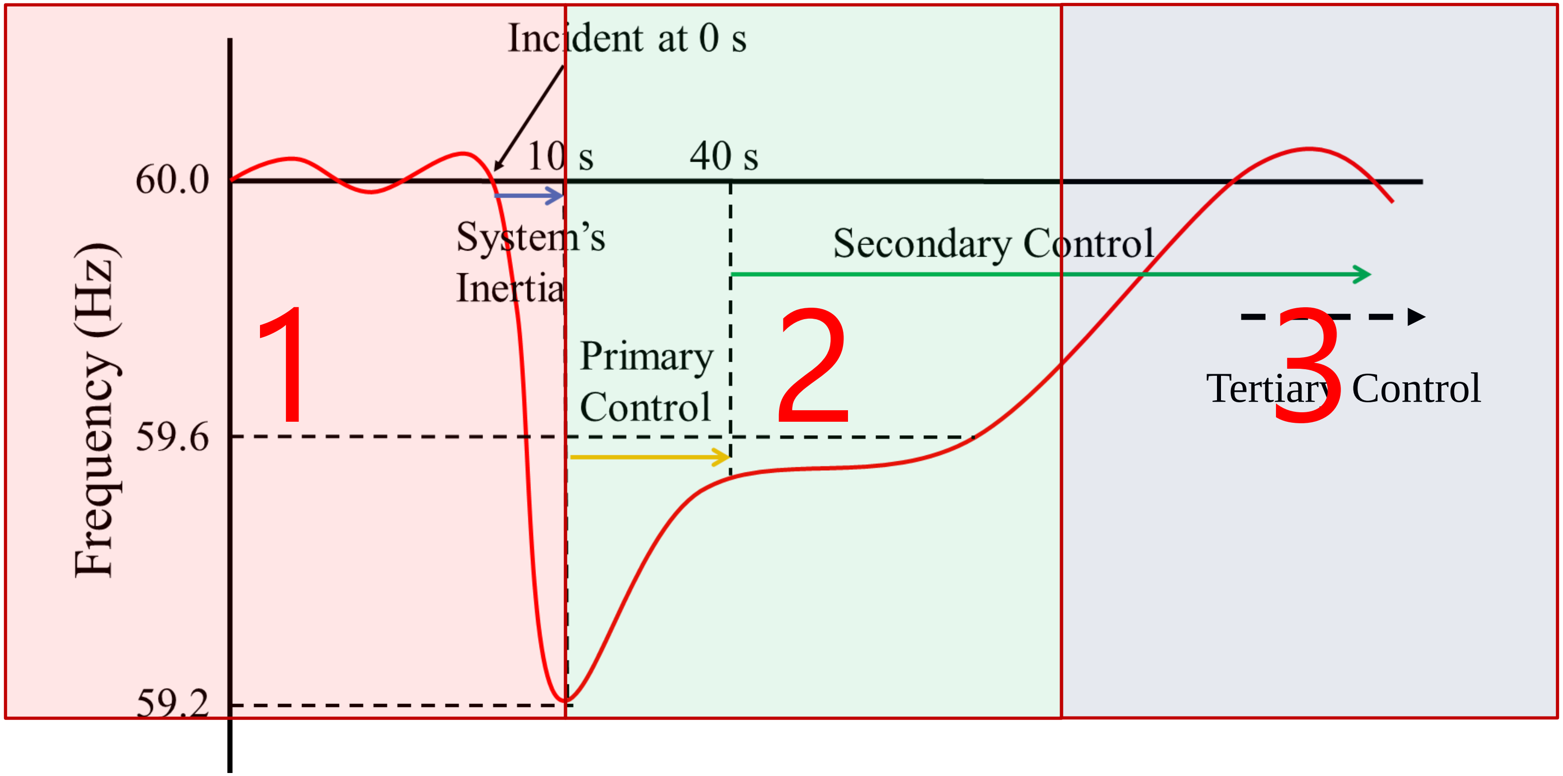
Manipulation of demand via IoT (MadIoT)

- High wattage IoT devices, once compromised, give the adversary a unique capability to ***manipulate the demand*** in the power grid



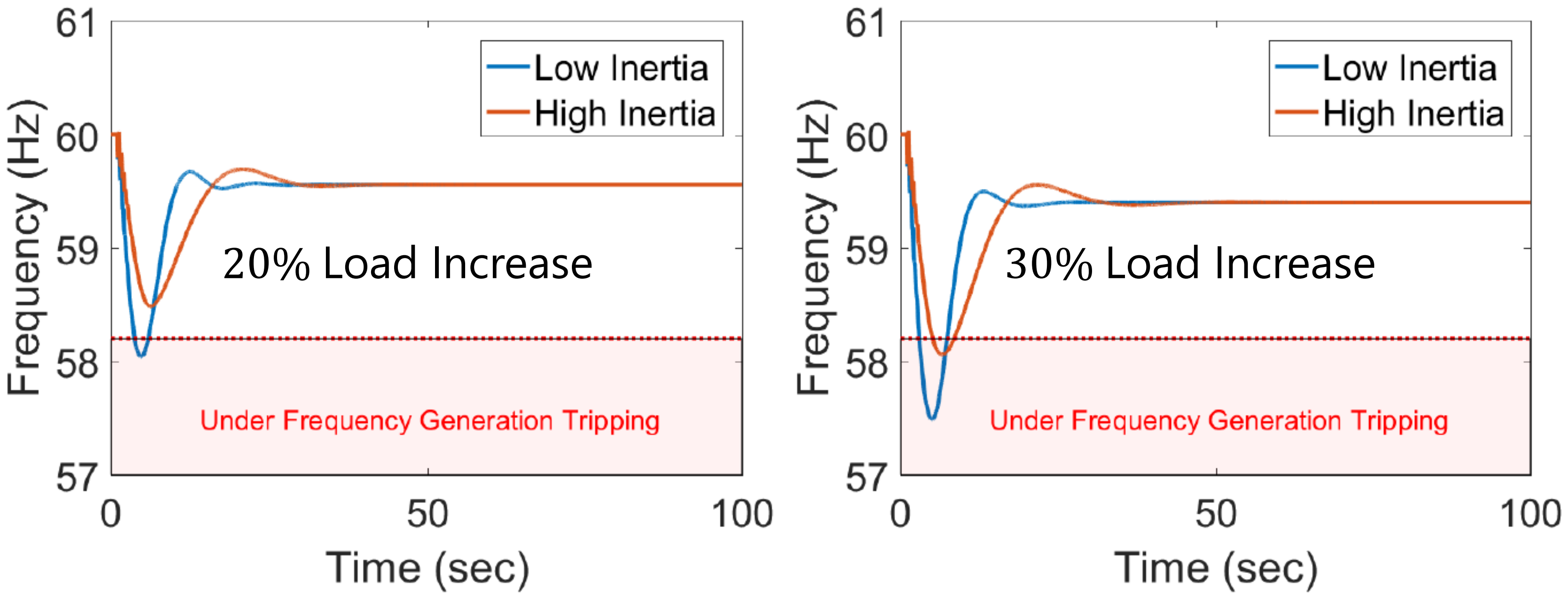
Consequences of MadIoT Attacks

- Different ways these attacks can disrupt normal operation of the grid:
  1. Result in the frequency instability
  2. Cause line failures and cascades (primary/secondary controller)
  3. Increase the operating cost (tertiary controller)



1 Causing Frequency Disturbance

- Frequency response of the WSCC 9-bus system after a MadIoT attack



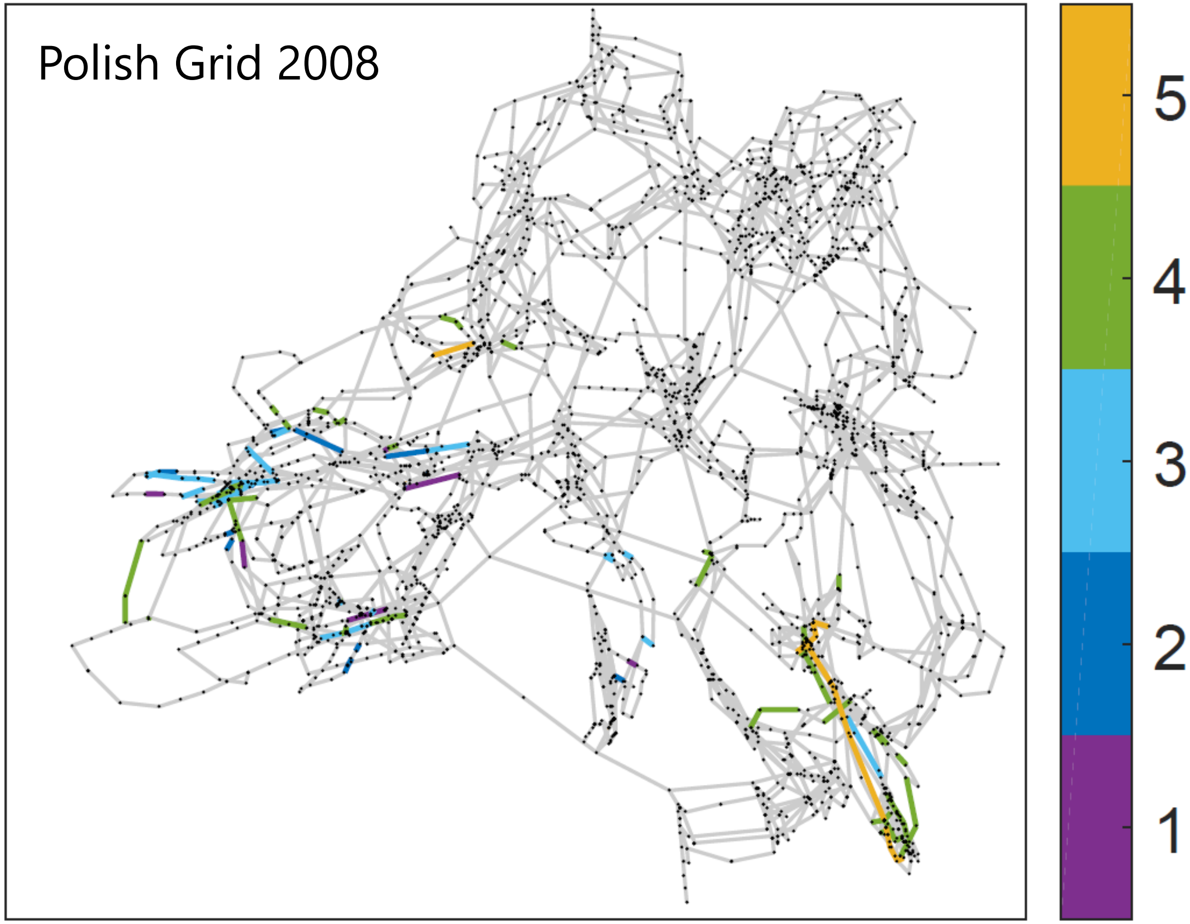
- Effectiveness of an attack depends on the *attack's scale* as well as the system's *total inertia* at the time of the attack

Sufficiently large simultaneous increase in the demand can result in a significant drop in the system's frequency and cause generation tripping

2 Initiating a Cascading Line Failures

- Sequence of line failures after *1% increase* in the demand in Polish grid 2008
  - Requires access to 210,000 smart ACs

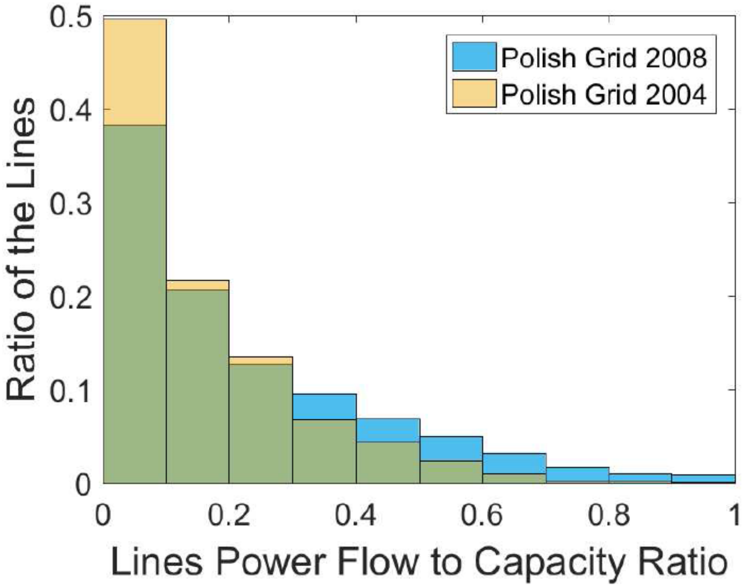
Only 1% increase in the demand in Polish grid 2008 initiates a cascading line failure resulting in 263 line failures and 86% outage



2 Cascading Failures (Critical Factor)

- An attack with similar consequences requires at least 10% increase in the demand in Polish grid 2004 → about *2 million smart ACs*

- Histogram of the Polish grid lines' power flow to capacity ratio in Summer 2004 compared to Summer 2008



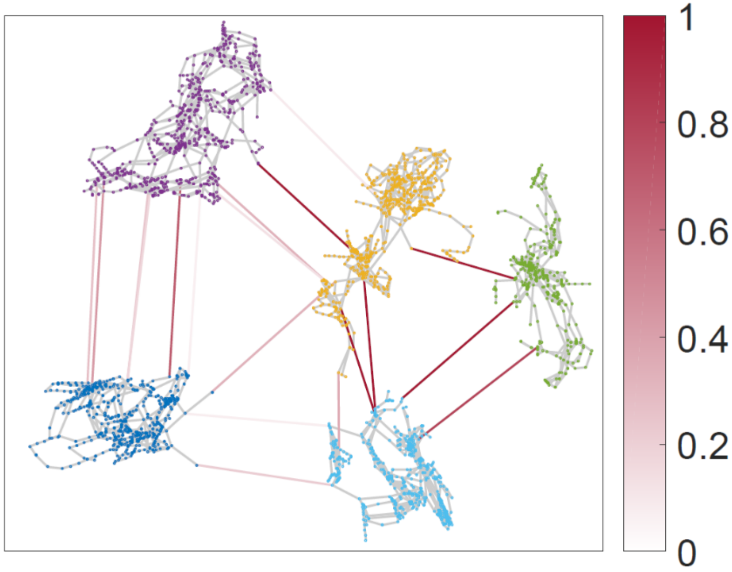
- It is important *how saturated the powerlines are* at the time of an attack

- *Attacks resulting in cascading line failures require fewer number of bots than the attacks resulting in critical frequency disturbances*

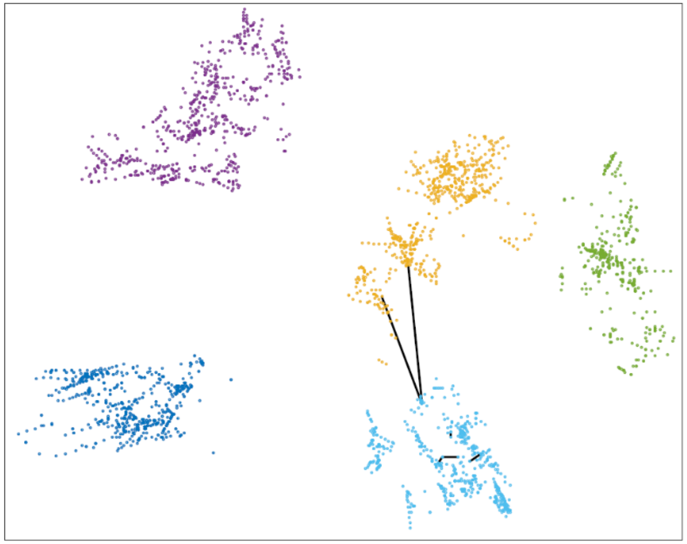
2

Overloading Tie-lines

- Tie-lines connect neighboring countries or states
- Increasing demand at the receiving region and decreasing the demand at the sending region of a tie-line (using IP addresses)



The ratios of tie-lines' power flows to their nominal capacity

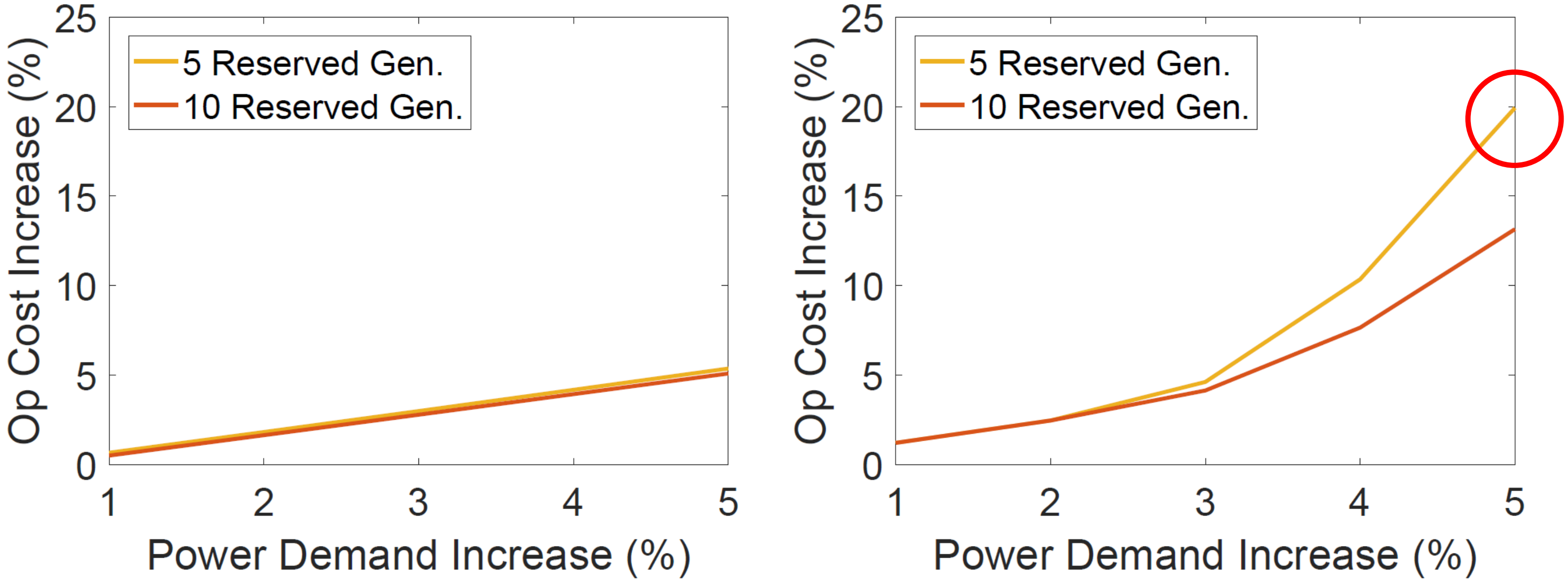


1.5% *increase* of demand in the yellow area and 1.5% *decrease* of demand in the blue area

By overloading a tie-line, an attacker can force it to trip resulting in significant imbalance between supply and demand in two neighboring areas and major frequency disturbances → Italy 2003 blackout

3 Increasing the Operating Cost

- Increasing the operating cost of the grid by forcing the operator to use [expensive] reserve generators
- An adversary’s attack may be for the benefit a particular utility in the electricity market rather than damaging the infrastructure



In certain situations, only 5% increase in the demand can result in 20% increase in the operating cost

Required Botnet Size Comparison

- Assuming all the bots are 1000W air conditioners

	Adversary's Goal	**Required Botnet size**
1	Critical frequency drop	200-300 bots/MW
2	Line failures and cascades	4-15 bots/MW
3	Increasing the operating cost	30-50 bots/MW

- *Estimates* based on only publicly and freely available test grids
  - May be different in grids with different characteristics
  - More detailed analysis on the effects of MadIoT attacks should be performed by system operators
- Substantial number of IoT devices are required to cause a significant drop in the frequency of the system
  - They should all be in the same geographical region
  - ACs have delay in reaching their maximum power (10-15 seconds)
- It is easier to achieve these numbers few years from now

Unique Properties of MadIoT Attacks

- ❑ *Indirect attacks* → no need to access the well-protected (?) SCADA

- ❑ *Very hard to detect and disconnect* by the grid operator → the security breach is in the IoT devices, yet the attack is on the power grid

- ❑ *Easy to repeat* → repeat until successful

- ❑ *Black-box* → An adversary does <u>not</u> need to know the underlying topology or the detailed operational properties of the grid

- ❑ *Power grids are not prepared to defend* against the MadIoT attacks → not part of the *contingency list*

Countermeasures

- *Improving the frequency stability of the system:*
  - The operators should account for possible attacks and require minimum spinning reserve such that grid has enough inertia at the time of an attack
  - Devices that provide virtual inertia such as flywheels, batteries, and super-capacitors can increase the total inertia of the system at a *lower cost*

- *Prevent line failures*
  - Operate the grid at an operating point such that after any potential attack no line gets overloaded
  - In general a nonconvex problem→ new paper to find such an operating point efficiently at https://arxiv.org/abs/1808.03826

- *Remove sensitive online data such as power flow on the tie-lines*

Conclusions

- Protecting the grid against MadIoT attacks requires efforts from researchers in *power systems* as well as *systems security* communities

  - **Power system's operators:** Rigorously analyze the effects of potential MadIoT attacks on their systems and develop preventive methods to protect the grid

  - **IoT Security:** Insecure IoT devices can have devastating consequences far beyond individual security/privacy losses → rigorous pursuit of security of IoT devices, including regulatory frameworks

  - **Interdependency:** Interdependency between infrastructure networks may lead to hidden vulnerabilities → System designers and security analysts should explicitly study threats introduced by interdependent infrastructure networks

Thank You!

ssoltan@princeton.edu
http://ssoltan.mycpanel.princeton.edu/

This work was supported in part by the U.S. National Science Foundation under Grants DMS-1736417, ECCS-1549881, and CNS-1553437, and Office of Naval Research YIP Award.