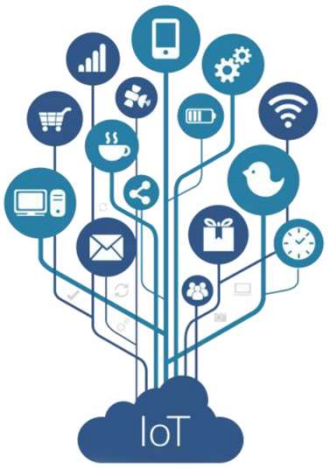
MANCHESTER 1824
The University of Manchester



COMP32412: Internet of Things Architecture and Applications

Case Study: Attacks on power grids

Mustafa A. Mustafa

mustafa.mustafa@manchester.ac.uk
KB 2.93, 2nd Floor, Kilburn Building

MANCHESTER 1824
The University of Manchester

Overview & Learning Outcomes

- Describe and identify attacks on power grids

MANCHESTER 1824
The University of Manchester

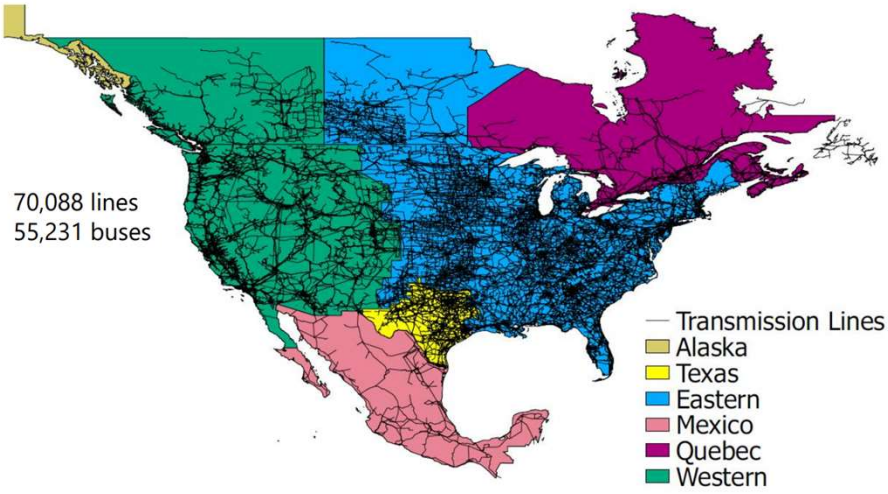
Power grid

765 kV-110 kV

34.5 kV-110 V

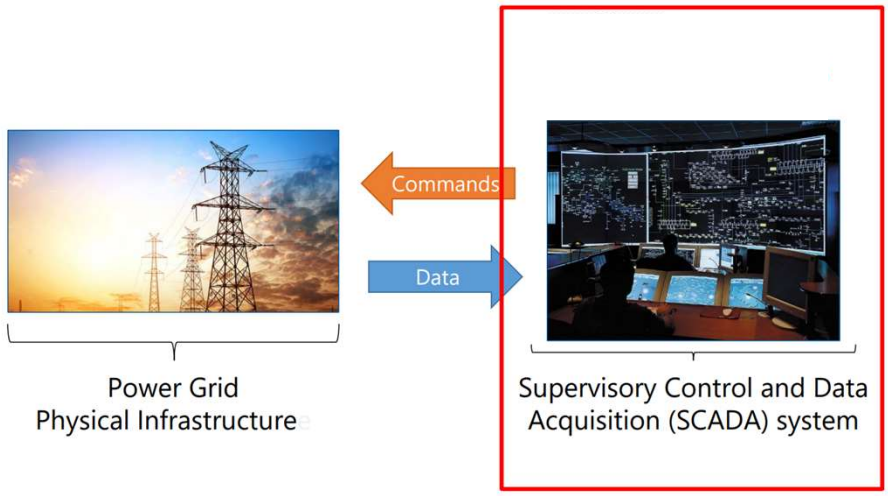
MANCHESTER 1824
The University of Manchester

North America Transmission Network



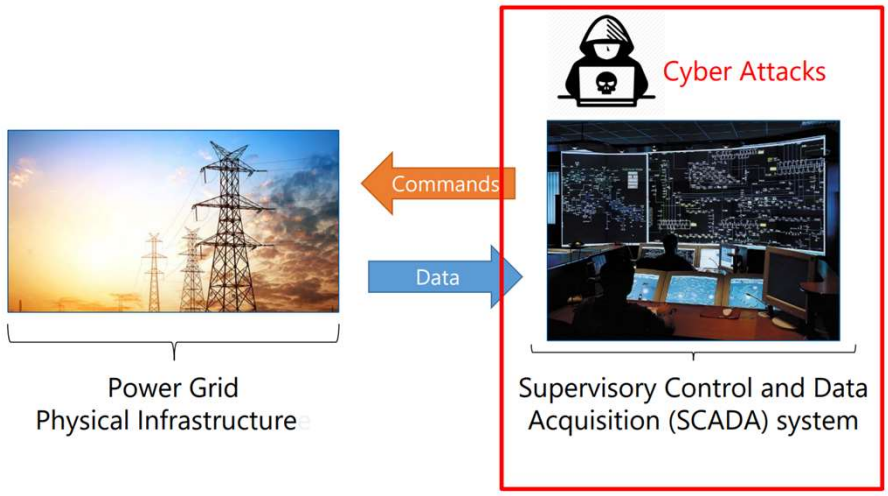
MANCHESTER 1824
The University of Manchester

SCADA system



MANCHESTER 1824
The University of Manchester

SCADA is a target



MANCHESTER 1824
The University of Manchester

Attacks on Ukraine's power grid 2015


BBC Sign in Home News Sport Weather

NEWS

Home | Israel-Gaza war | Cost of Living | War in Ukraine | India Election | Climate |

Technology

Hackers caused power cut in western Ukraine - US

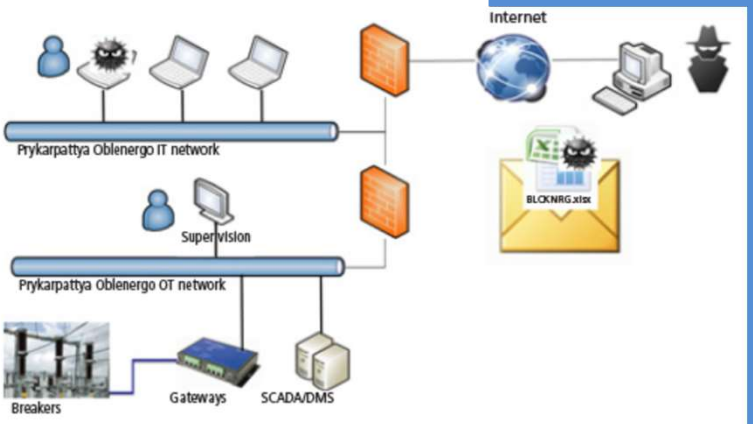
12 January 2016

MANCHESTER 1824
The University of Manchester

Attack on Ukraine's power grid 2015

Preparation

- Phishing: malicious Word/Excel document sent to workers via emails
  - Asked macros to be enabled
- Malware injection: BlackEnergy3 installed in the IT network



8

- Phishing: The phishing campaign delivered email to workers at three of the companies with a malicious Word document attached. When workers clicked on the attachment, a popup displayed asking them to enable macros for the document. If they complied, a program called BlackEnergy3---variants of which have infected other systems in Europe and the US---infected their machines and opened a backdoor to the hackers. This got the attackers only as far as the corporate networks. But they still had to get to the SCADA networks that controlled the grid. The companies had wisely segregated those networks with a firewall, so the attackers were left with two options: either find vulnerabilities that would let them punch through the firewalls or find another way to get in. They chose the latter.

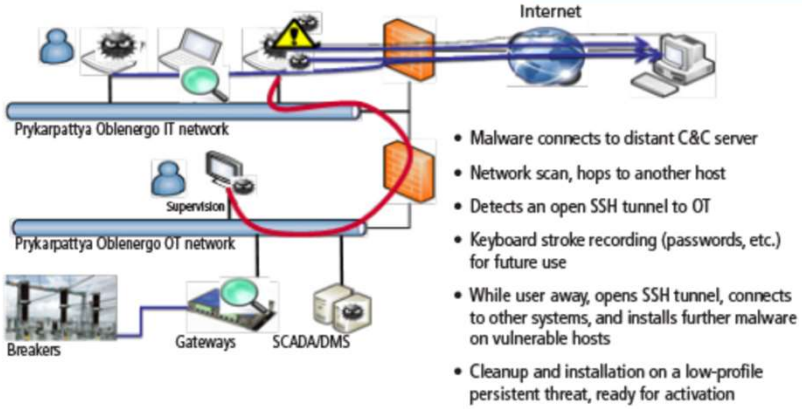
Source
- Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid | WIRED
- Special Section: Ukrainian power grids cyberattack – ISA

MANCHESTER 1824
The University of Manchester

Attack on Ukraine's power grid 2015

Preparation

- Intelligence gathering – 8 months
  - Harvested worker credentials, some of them for VPNs the grid workers used to remotely log in to the SCADA network.
- Reconfigured UPS used for backup power to control centers.
- Wrote malicious firmware to replace the legitimate firmware on serial-to-Ethernet converters at more than a dozen substations



9

- Over many months they conducted extensive reconnaissance, exploring and mapping the networks and getting access to the Windows Domain Controllers, where user accounts for networks are managed. Here they harvested worker credentials, some of them for VPNs the grid workers used to remotely log in to the SCADA network. Once they got into the SCADA networks, they slowly set the stage for their attack.
- First they reconfigured the uninterruptible power supply[1], or UPS, responsible for providing backup power to two of the control centers. When power went out for the wider region they wanted operators to be blind, too.
- Then they wrote malicious firmware to replace the legitimate firmware on serial-to-Ethernet converters at more than a dozen substations (the converters are used to process commands sent from the SCADA network to the substation control systems). Taking out the converters would prevent operators from sending remote commands to re-close breakers once a blackout occurred. Operation-specific malicious firmware updates [in an industrial control setting] has *never* been done before.

Source

- Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid | WIRED
- Special Section: Ukrainian power grids cyberattack – ISA

MANCHESTER 1824
The University of Manchester

Attack on Ukraine's power grid 2015

The attack

- Entered SCADA through the hijacked VPNs
- DoS on the telephone system – flooded with thousand bogus calls
- Disabled UPS systems
- Open breakers (Breaker connects power sources to the grid)
- False data injection: Remote Monitoring Units were reporting false data
- Overwrote firmware on some of the substation serial-to-Ethernet converters
- Used KillDisk malware to wipe files from operation stations

10

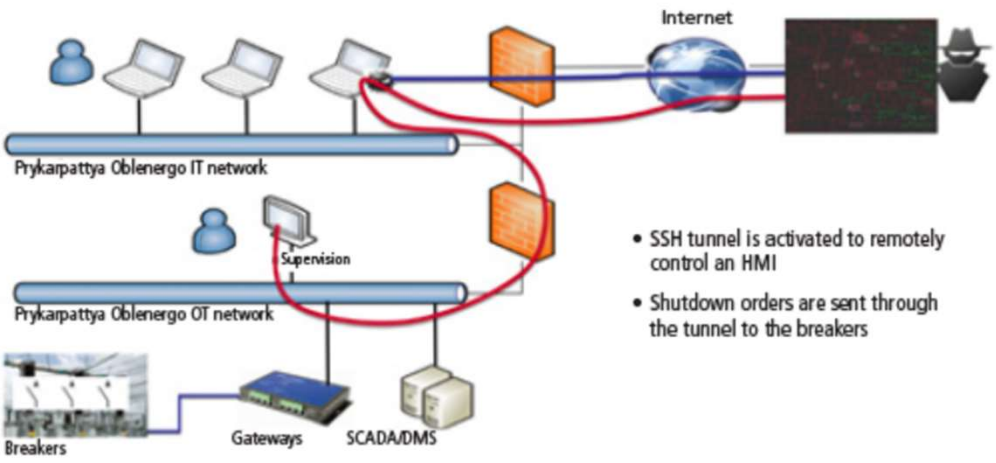
- Sometime around 3:30 p.m. on December 23 they entered the SCADA networks through the hijacked VPNs and sent commands to disable the UPS systems they had already reconfigured.
- But before they did, they launched a telephone denial-of-service attack against customer call centers to prevent customers from calling in to report the outage. The center's phone systems were flooded with thousands of bogus calls that appeared to come from Moscow, in order to prevent legitimate callers from getting through.
- Then they began to open breakers.
- As the attackers opened up breakers and took a string of substations off the grid, they also overwrote the firmware on some of the substation serial-to-Ethernet converters, replacing legitimate firmware with their malicious firmware and rendering the converters thereafter inoperable and unrecoverable, unable to receive commands.
- After they had completed all of this, they then used a piece of malware called KillDisk to wipe files from operator stations to render them inoperable as well. KillDisk wipes or overwrites data in essential system files, causing computers to crash. Because it also overwrites the master boot record, the infected computers could not reboot.

Source

- Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid | WIRED

MANCHESTER 1824
The University of Manchester

Attack on Ukraine's power grid 2015



- SSH tunnel is activated to remotely control an HMI
- Shutdown orders are sent through the tunnel to the breakers

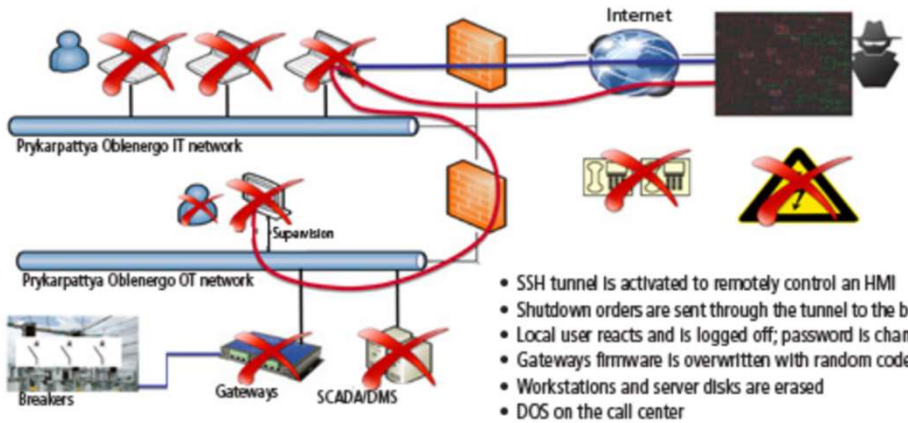
11

Source

- Special Section: Ukrainian power grids cyberattack – ISA

MANCHESTER 1824
The University of Manchester

Attack on Ukraine's power grid 2015



- SSH tunnel is activated to remotely control an HMI
- Shutdown orders are sent through the tunnel to the breakers
- Local user reacts and is logged off; password is changed
- Gateways firmware is overwritten with random code
- Workstations and server disks are erased
- DOS on the call center
- UPS are shut down

12

Source

- Special Section: Ukrainian power grids cyberattack – ISA

MANCHESTER 1824
The University of Manchester

Attack on Ukraine's power grid 2015

The damage

- 200K+ households without electricity for 1-3 hours
- Converters were inoperable and unrecoverable, unable to receive commands
- Remote control of switches was not possible, requiring manual switching for months
- Many breakers and switches had to be replaced

MANCHESTER 1824
The University of Manchester

Attacks on Ukraine's power grid 2016

Ukraine's Power Grid Gets Hacked Again, a Worrying Sign for Infrastructure Attacks

Russian hackers may be behind attacks leveled at the nation's power grid and artillery. The West should take note.

By Jamie Condliffe

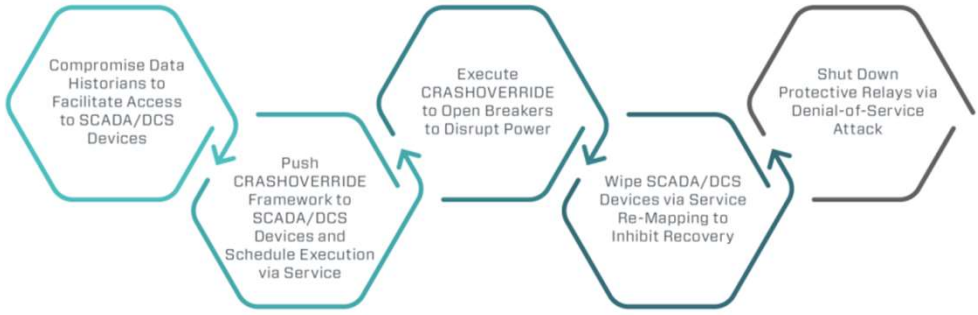
December 22, 2016

The University of Manchester

Attack on Ukraine's power grid 2016

CRASHOVERRIDE

- Resulted in 1h blackout – less severe than 2015 attack
- Failed in its main goal – to shut protective relays



15

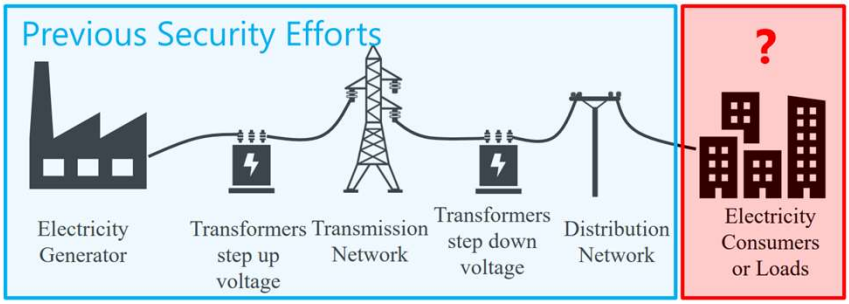
Source

- [CRASHOVERRIDE: Reassessing the 2016 Ukraine Electric Power Event as a Protection-Focused Attack (dragos.com)]

MANCHESTER 1824
The University of Manchester

Smart gird attack vectors

- 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?



16

- 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?

MANCHESTER 1824
The University of Manchester

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

- 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!

17

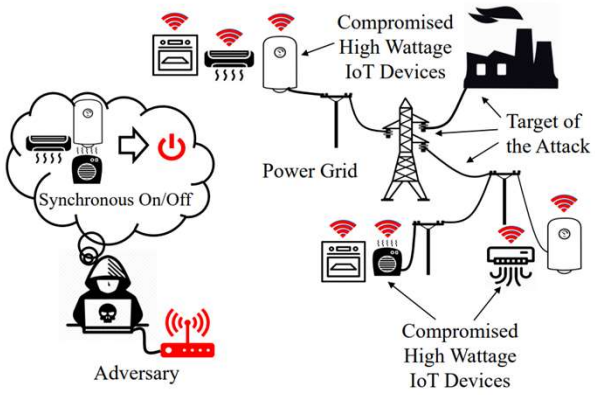
Source

- Soltan, Saleh, Prateek Mittal, and H. Vincent Poor. "{BlackIoT}:{IoT} botnet of high wattage devices can disrupt the power grid." *27th USENIX Security Symposium (USENIX Security 18)*. 2018.

MANCHESTER 1824
The University of Manchester

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

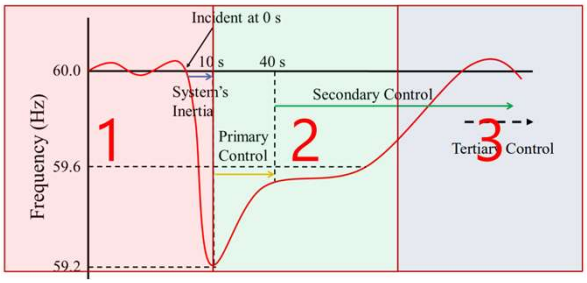


MANCHESTER 1824
The University of Manchester

Consequences of MadIoT Attacks

Different ways these attacks can disrupt normal operation of the grid:

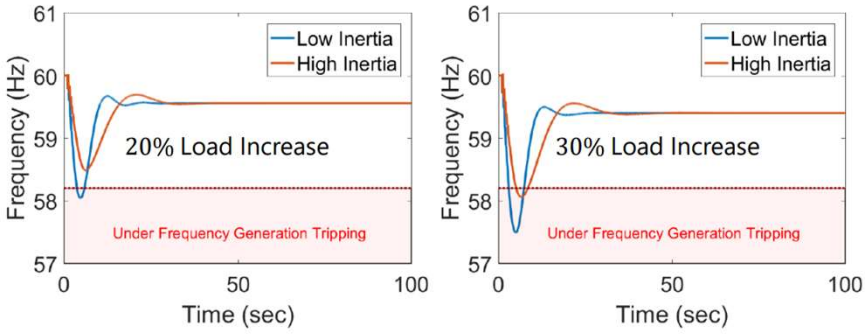
1. Result in the frequency instability
2. Cause line failures and cascades (primary/secondary controller)
3. Increase the operating cost (tertiary controller)



MANCHESTER 1824
The University of Manchester

Causing Frequency Disturbance

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



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

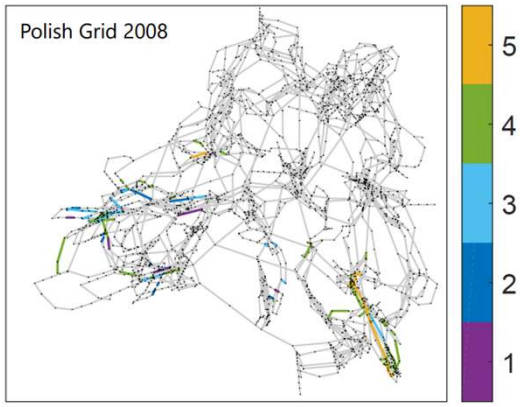
MANCHESTER 1824
The University of Manchester

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

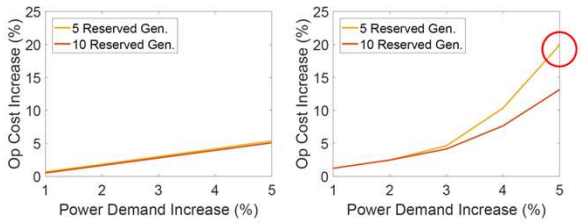
Only 1% increase in the demand in Polish grid 2008 initiates a cascading line failure resulting in 263 line failures and 86% outage



MANCHESTER 1824
The University of Manchester

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

MANCHESTER 1824
The University of Manchester

Required Botnet Size Comparison

	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

MANCHESTER 1824
The University of Manchester

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 not 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*

MANCHESTER 1824
The University of Manchester

Summary

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

- Power system's operators: Rigorously analyze the effects of potential 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