CREDC

CYBER RESILIENT ENERGY DELIVERY CONSORTIUM

Seminar Series

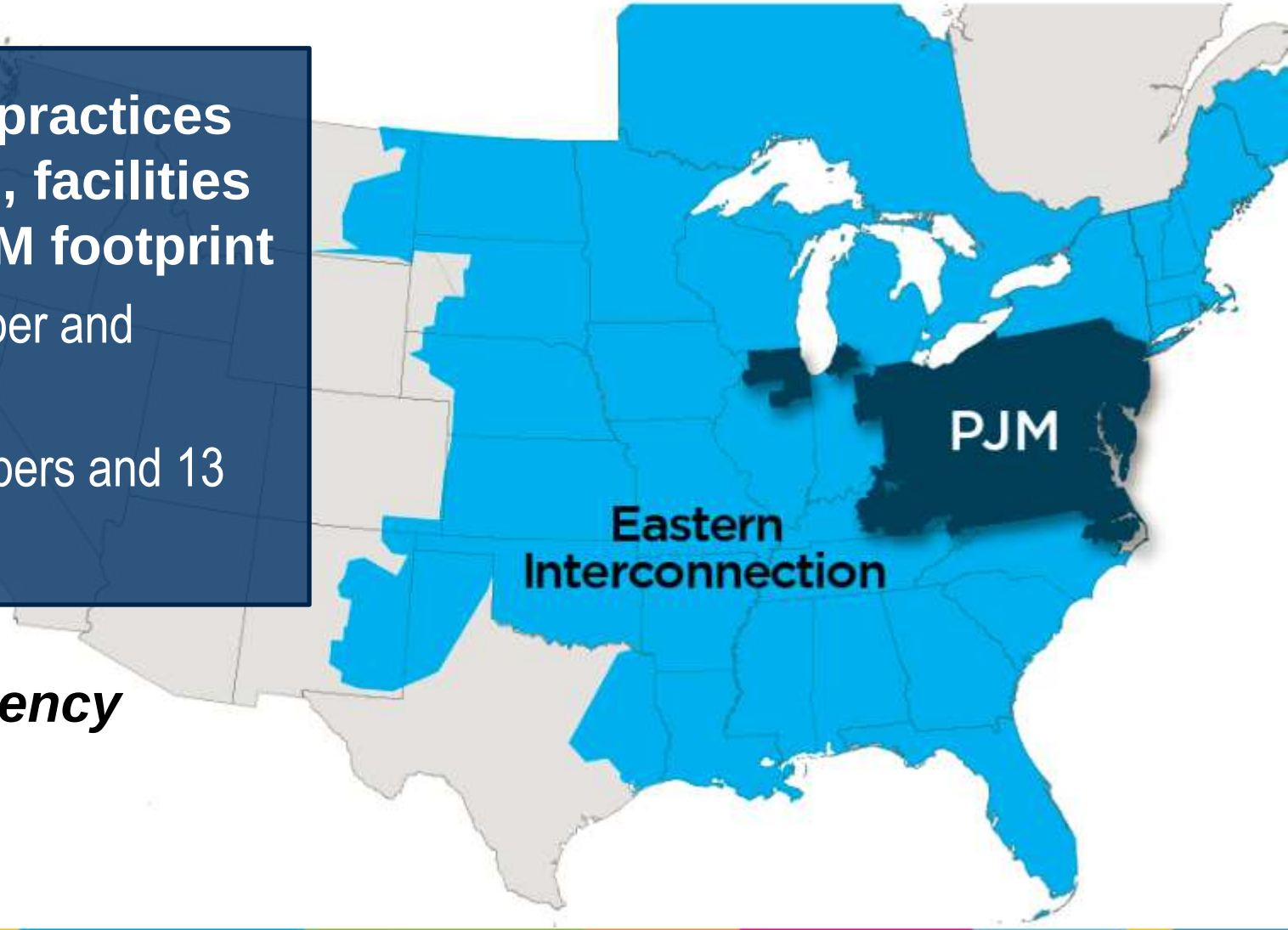
Black Sky Resilience: Cyber

Jonathon Monken
Senior Director, System Resiliency
PJM Interconnection

Security and Resilience Paramount

Cyber and physical security practices protect information, systems, facilities and the people within the PJM footprint

- PJM entrusted with critical member and market data
- Connected to nearly 1,000 members and 13 states + D.C.



From reliability and efficiency to system resilience

Lynchpins

5,600 substations
2.5-5% critical

Operation of the Energy Management System

Generation is rarely affected

Requires visibility and connectivity

Single-feed transmission vulnerability

What is Black Sky Hazard?

Threats

Nation state threats

Un-attributable threat actors

Insider threats

Additional man-made or natural events

Un-attributable Threats & Criminal Behavior: Metcalf Substation Attack

Pacific Gas and Electric's Metcalf Substation

When	April 2013
Where	San Jose, Calif.
Attribution	Criminal individuals
Methods	Coordinated physical attack
Impacts	$15 million in substation repairs

Superstorm Sandy: A Tale of Extremes

When	October 2012
Where	Coast to Appalachians
Impacts	Damage from floods, winds and snow $63 billion in economic impact 4.8 million people affected

Natural Events: 1989 Geomagnetic Storm

Powerful Solar Storm Causes Blackout in Quebec

When	March 1989
Where	Quebec, some U.S. impacts
Impacts	Blackout throughout Quebec About $1 billion economic impact 200 power grid problems noted in U.S.

Salem Nuclear Plant GSU Transformer Failure, March '89

Man-made or Natural Events: 2003 Northeast Blackout

Originating in Ohio, Blackout Affects U.S. Northeast and Parts of Canada

Not a security or natural event, but an operational failure

When	August 2003
Where	Northeast U.S. and Canada
Duration	Up to two days
Impacts	508 generating facilities offline 55 million people affected Economic cost: $7-$10 billion

Un-attributable Threats: Ukraine Power Grid Cyber Attack

First Successful Cyberattack on a Power Grid*

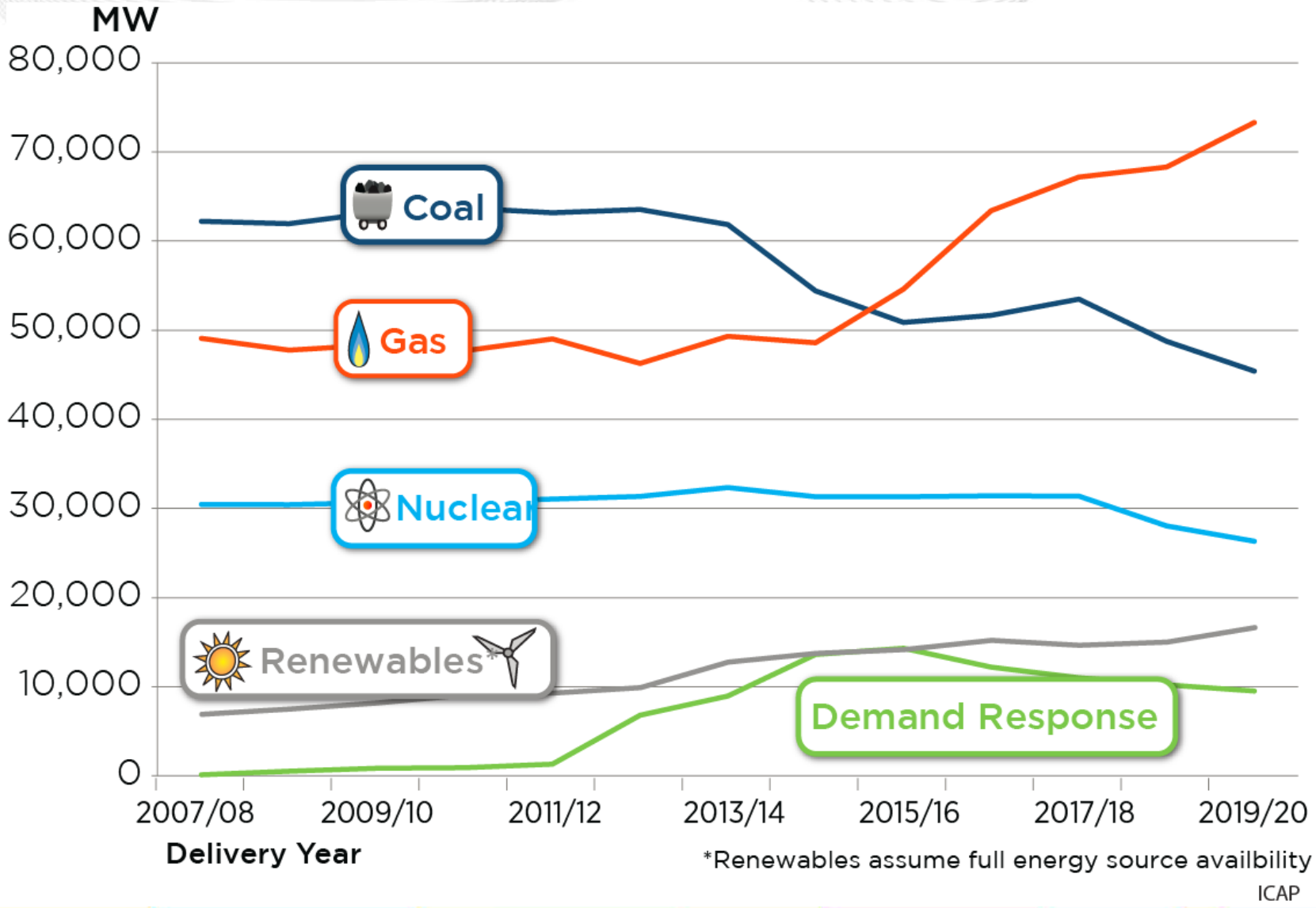
When	December 2015
Where	Ukraine
Attribution	Unknown
Methods	Denial-of-service attacks, phishing, malware
Impacts	134 MW load lost 225,000 people affected

* Details and attribution vary from different sources

Vital Interdependencies

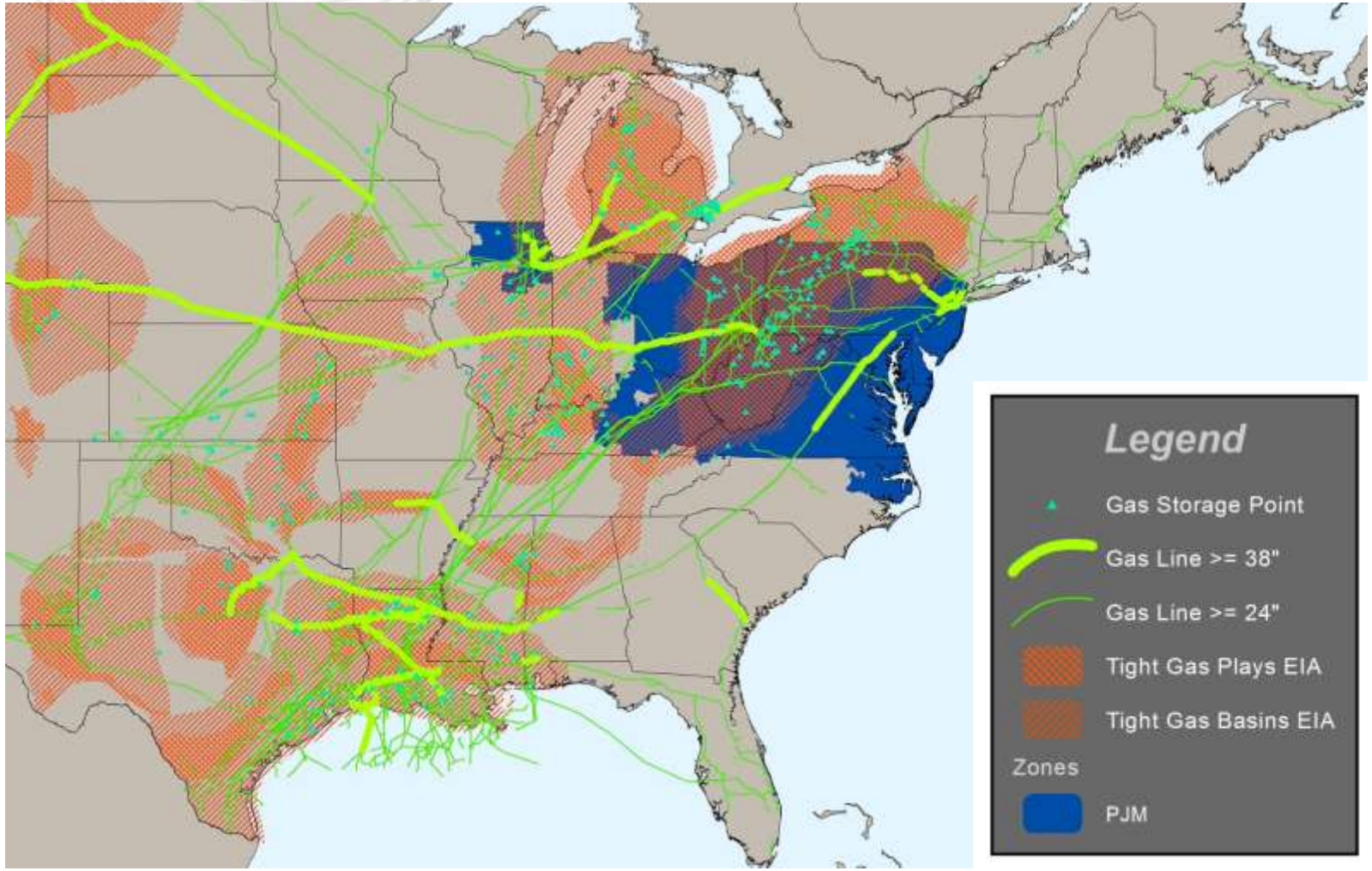
Natural Gas a Generation Fuel Source

- Relies on just-in-time delivery
- Opposing trends for natural gas vs. coal
- Disproportionate number of natural gas black start plants
- Few plants with ‘firm’ contracts



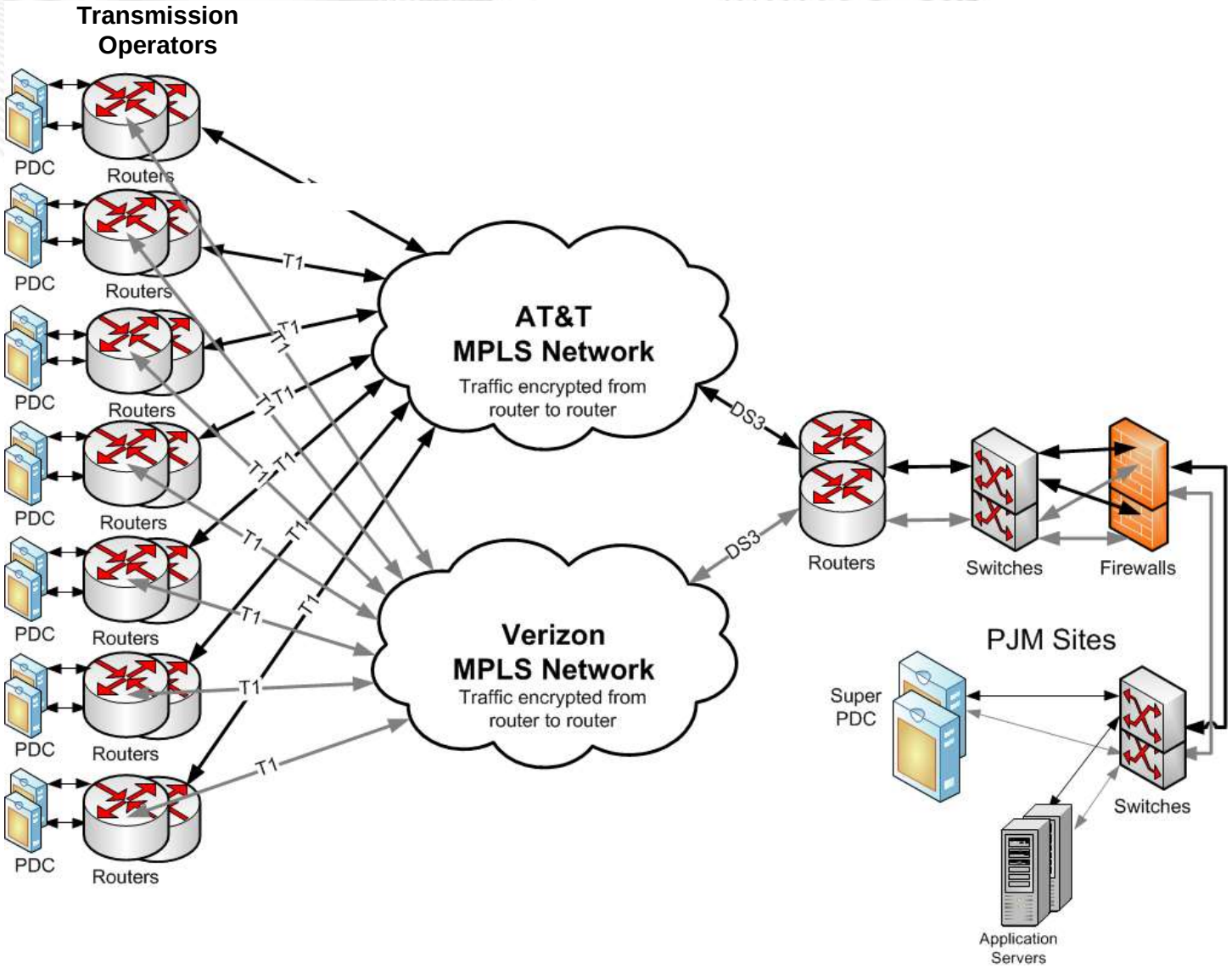
Natural Gas Distribution

- Growing number electricity-powered compressors
- Fewer system redundancies, less coordination
- Longer repair times
- Limited storage



Communications

- Essential for grid and market operations
- Heavily dependent on commercial systems
- Extensive shared physical infrastructure



Two-way Street

- 24 hours of back-up power
- Few alternative mediums for communication
- ‘Manual’ operation of the grid

From Reliability to Resilience

So what happens if…

Widespread, long duration outage

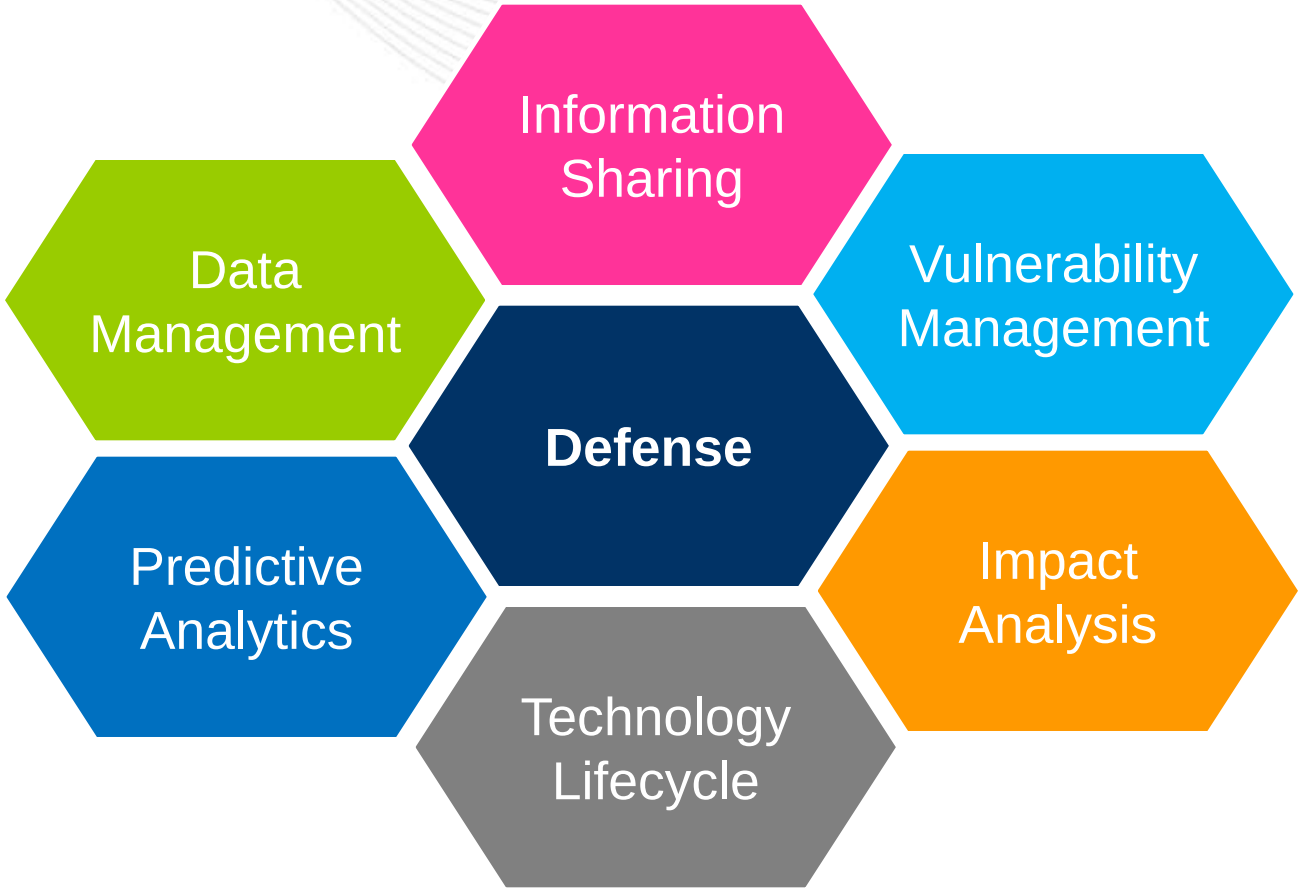
Natural vs. malicious

The challenges of scale

- Situational Awareness
- Communications
- Prioritization

Critical, low-density engineering assets

Defense



Government Sources

Situational Awareness

Industry Sources

Commercial Sources

Cyber Resilience

- PJM has two systems that are able to control the power grid in the event the EMS systems at both sites (AC1 – Jefferson and AC2 – Milford) fail simultaneously
- The systems are referred to as:
  - Golden Image
  - Virtual Backup Control Center
- Each of these systems has different characteristics to mitigate the effects of different types of failures

Golden Image Purpose

Intended to mitigate the effects of a *cyberattack* that compromises all other PJM systems

Is ‘air gapped’ from all other systems (except when in use or being updated)

Can run the power grid for a long period of time (days)

Will usually be ‘back level’ and have multiple older images to select from

VBUCC Purpose

Mitigates the effects of a **dual failure** that compromises both of PJM's EMS systems,
e.g., a database update gone wrong, hardware failure, cyber intrusion…etc.

Designed to come up quickly (minutes)

Today is in production as a backup ACE calculator.
(Includes independent data feed for ACE related telemetry)

Capable of running a full EMS including Advanced Applications

Cyber Mutual Assistance

- Three types available
  - Industry to Industry (ESCC CMA)
  - Private Sector to Industry (Contract)
  - Government to Industry (ICS-CERT)
- Lane de-confliction
- Cross-training and exercise
- Governance challenges

Emerging Opportunities

- “Packaged” threat and vulnerability INTEL sharing
  - Attribution, product, TTPs, malware, etc.
- Joint Intelligence Generation
  - Honeypots, sinkholes
- R&D Support for Tools and Capabilities
  - RADICS, Labs, ESCC
- Intra-sector Information Sharing
- DoD Partnerships

Security and Resilience is Paramount