Cambridge Centre for Risk Studies

Research Showcase 22 June 2015

UNDERSTANDING CYBER RISK

Simon Ruffle

Director of Research and Innovation

Centre for Risk Studies

Centre for **Risk Studies**

UNIVERSITY OF CAMBRIDGE Judge Business School

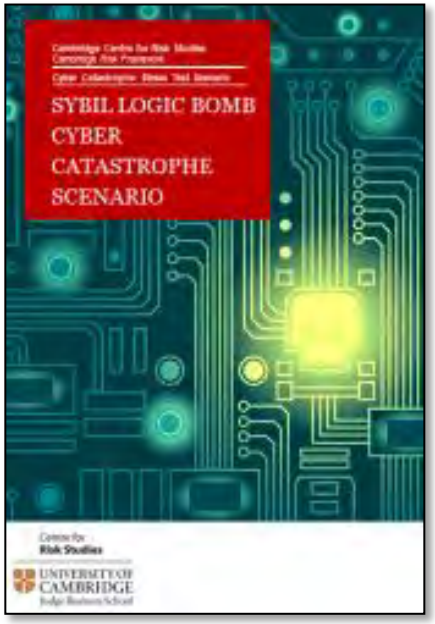
CJBS 25

Cyber Research Projects

- **'Sybil Logic Bomb' Stress Test Scenario**
  - First exploration of potential loss correlation in 'cyber catastrophe'
- **Risk Atlas of Global Cyber Risk**
  - World city risk of economic disruption from cyber
- **'Erebos Cyber Blackout' Stress Test Scenario**
  - Cyber attack on US Power Grid
  - Lloyd's Report – available July
- **Cyber Attack on UK Power Grid Stress Test Scenario**
  - Scenario in development for UK Power Grid
- **Cyber Aggregation Framework**
  - Cyber exposure and multiple scenarios of cyber PMLs

Sybil Logic Bomb Cyber Stress Test Scenario

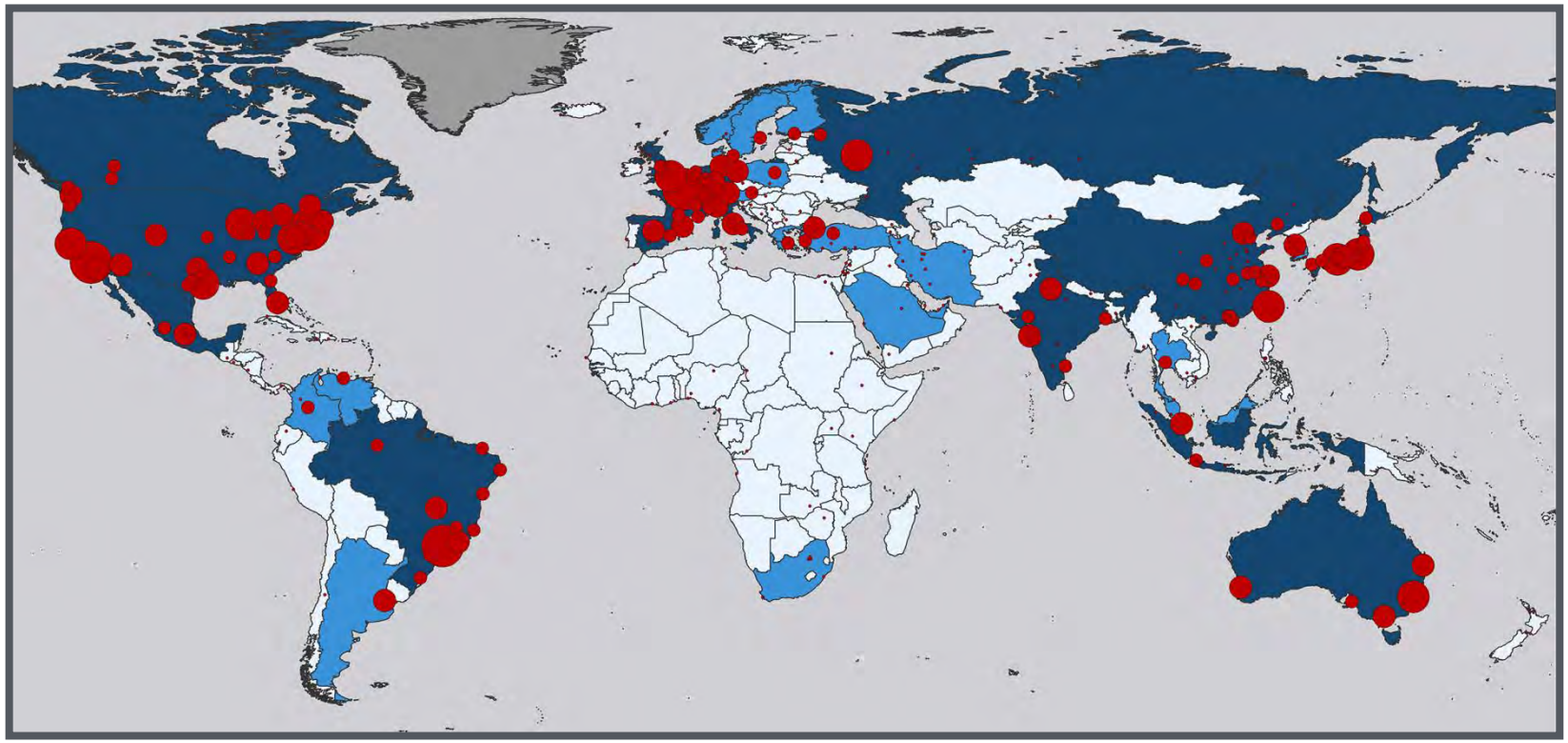
- Introduced key research concepts
  - Network Model of the Cyber Economy
  - Impact by Industry Sectors
  - Systemically Important Technology Enterprises
- Widely disseminated
- Used as a stress test in insurance industry
- Controversial



Cyber Research Projects

- **'Sybil Logic Bomb' Stress Test Scenario**
  - First exploration of potential loss correlation in 'cyber catastrophe'
- **Risk Atlas of Global Cyber Risk**
  - World city risk of economic disruption from cyber
- **'Erebos Cyber Blackout' Stress Test Scenario**
  - Cyber attack on US Power Grid
  - Lloyd's Report – available July
- **Cyber Attack on UK Power Grid Stress Test Scenario**
  - Scenario in development for UK Power Grid
- **Cyber Aggregation Framework**
  - Cyber exposure and multiple scenarios of cyber PMLs

Cities at Risk: Cyber Catastrophe



- Cyber Threat GDP@Risk for 300 cities

Cyber Research Projects

- **'Sybil Logic Bomb' Stress Test Scenario**
  - First exploration of potential loss correlation in 'cyber catastrophe'
- **Risk Atlas of Global Cyber Risk**
  - World city risk of economic disruption from cyber
- **'Erebos Cyber Blackout' Stress Test Scenario**
  - Cyber attack on US Power Grid
  - Lloyd's Report – available July
- **Cyber Attack on UK Power Grid Stress Test Scenario**
  - Scenario in development for UK Power Grid
- **Cyber Aggregation Framework**
  - Cyber exposure and multiple scenarios of cyber PMLs

Erebos US Cyber Blackout Stress Test Scenario

Centre for Risk Studies

UNIVERSITY OF CAMBRIDGE
Judge Business School

LLOYD'S

Erebos Cyber Blackout Stress Test Scenario: Aurora Vulnerability

- Idaho National Laboratory 2007
- A generator remotely forced out of phase with the power grid by a cyber attack
- Compromise in either the protection relay or control signal
- Damage to the bushings, bearings, and coupling of the generator
- Generator was badly damaged and functionally unable to supply power to bulk power system
- www.youtube.com/watch?v=fJyWngDco3g

Erebos US Cyber Blackout Stress Test Scenario

- Malware is introduced into electricity generator control rooms
- Coordinated simultaneous attack targetted at two zones of United States power grid (NYISO & PJM)
- Malware finds 50 generators that it can control, and forces them to overload and burn out, in some cases causing additional fires and explosions
- Electricity blackout that plunges 15 US states and Washington DC into darkness
- 93 million people without power.
- More than 17 TW-Hours of generation is lost – around 12% of supply

Impacts of Power Outage

- Many companies and commercial activities unable to operate
- Offices and stores closed
- Public transport doesn't run
- Roads are unsafe due to signalling failures
- Many large facilities have backup generators, however as the blackout duration continues for some weeks in many parts of the region, fuel for generators becomes scarce.
- Social impact of the blackout is also severe


The New York Times

NEW YORK, FRIDAY, AUGUST 15, 2003

ONE DOLLAR

POWER SURGE BLACKS OUT NORTHEAST, HITTING CITIES IN CANADA AND 8 STATES; MIDDAY SHUTDOWNS DISRUPT MILLIONS

OVERLOADED GRID

Buildings Are Evacuated and Hospitals Fill — Bush Plans Review

Geographical Footprint of the Power Outage

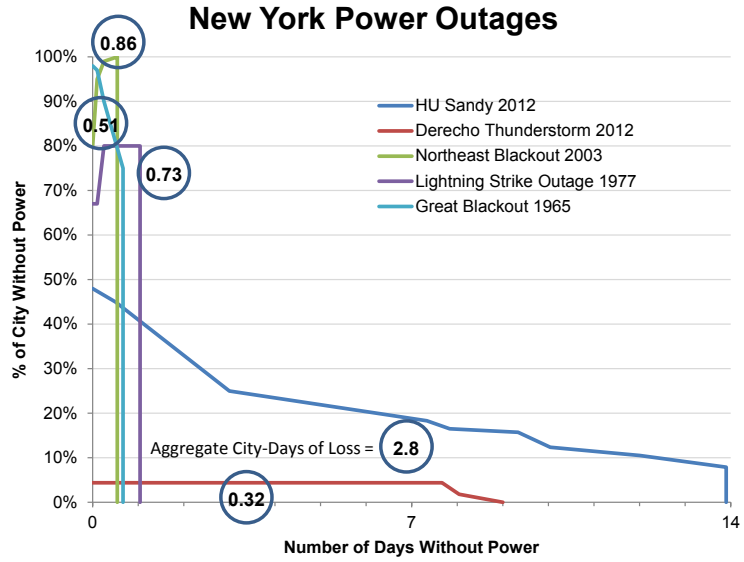
The outage impacts all companies and population in the following 15 US States + DC

- Connecticut
- Maine
- Massachusetts
- New Hampshire
- New York
- Rhode Island
- Vermont
- Delaware
- Indiana
- Maryland
- Michigan
- New Jersey
- Ohio
- Pennsylvania
- West Virginia

- District of Columbia

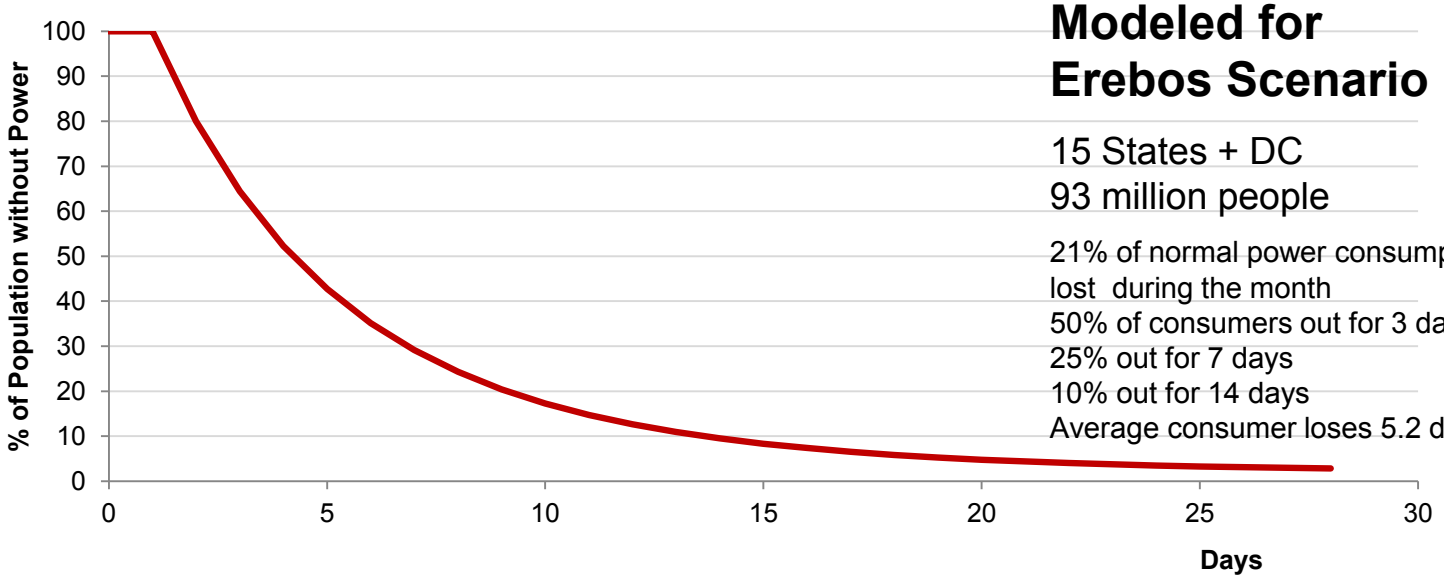
Total population of the impacted region: **93 million**
30% of US population and 32% of US GDP

Outage & Restoration of Power



Historical Examples

New York
8 million people

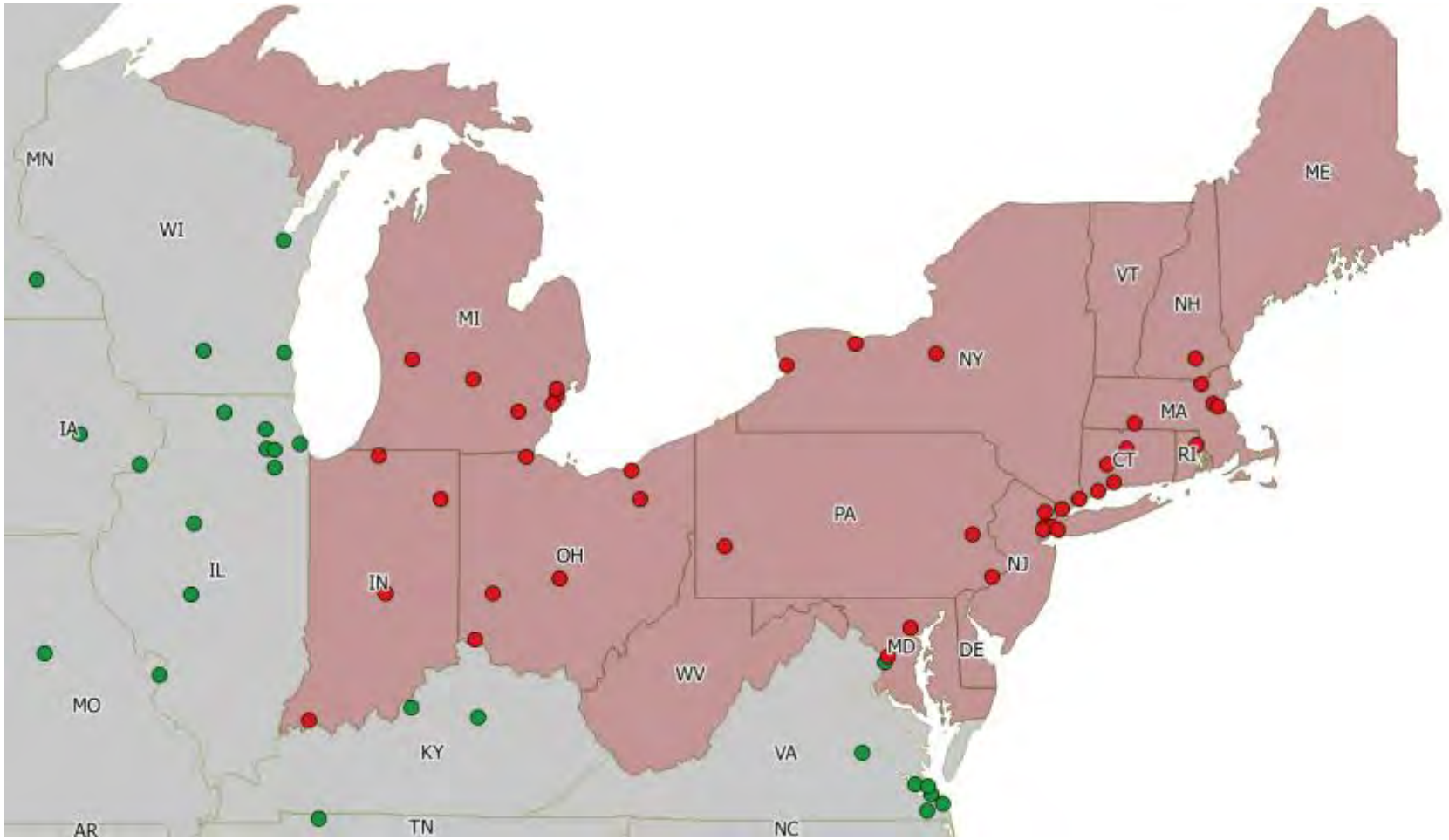


Modeled for Erebos Scenario

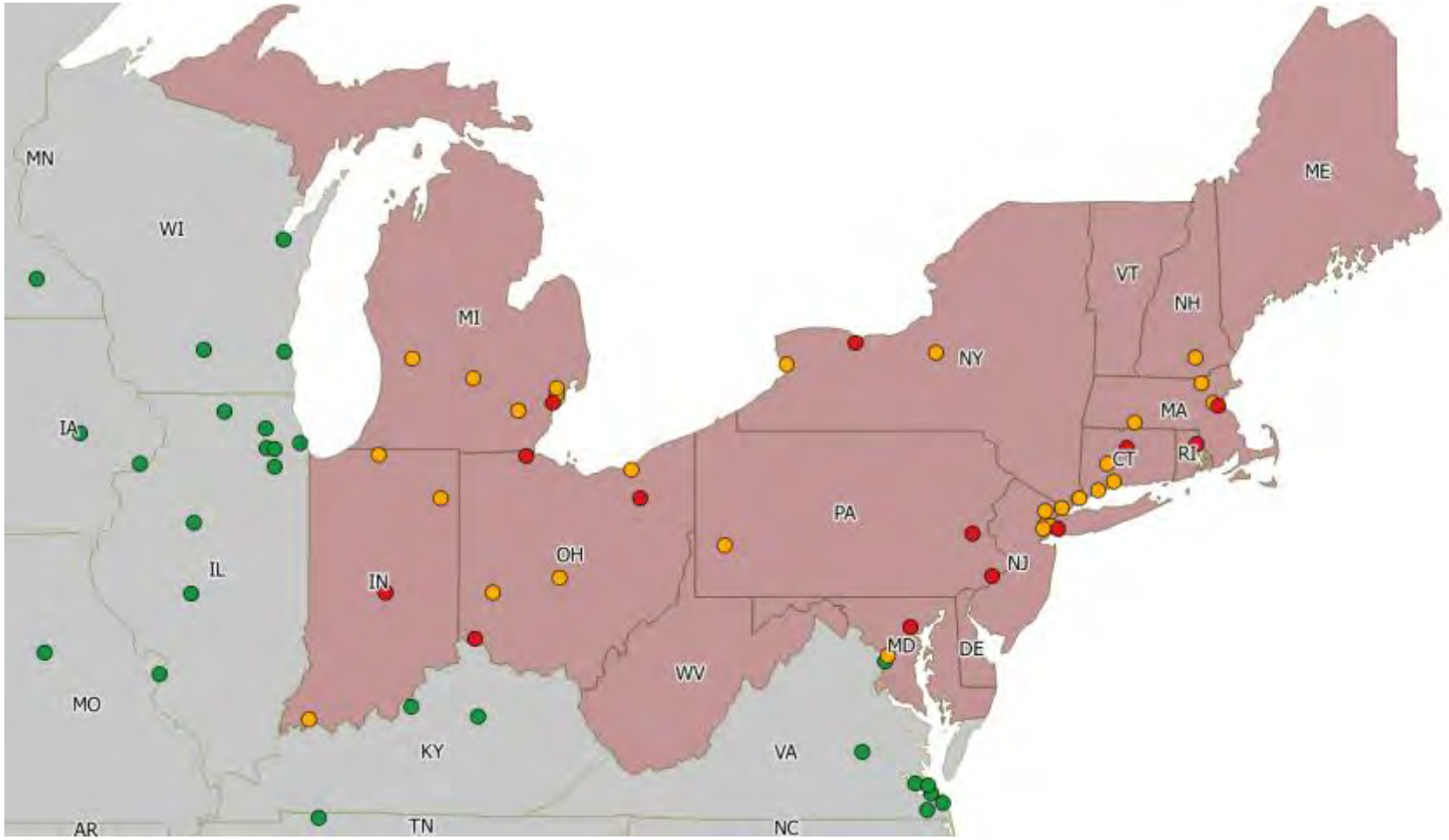
15 States + DC
93 million people

21% of normal power consumption lost during the month
50% of consumers out for 3 days
25% out for 7 days
10% out for 14 days
Average consumer loses 5.2 days

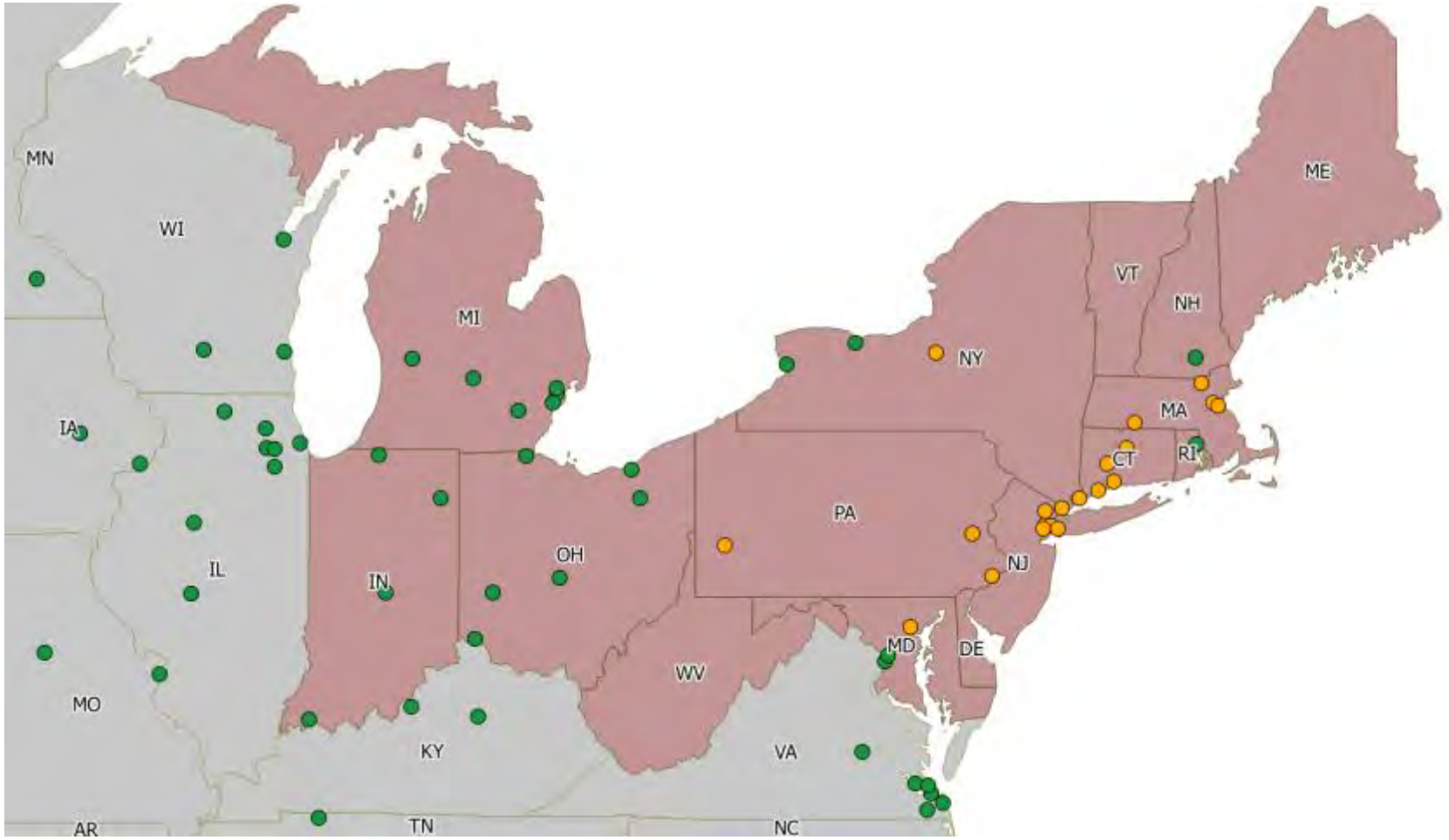
Day 0


MN
WI
MI
IA
IL
IN
OH
MO
KY
WV
VA
AR
TN
NC
PA
NY
MD
DE
NJ
CT
RI
MA
VT
NH
ME

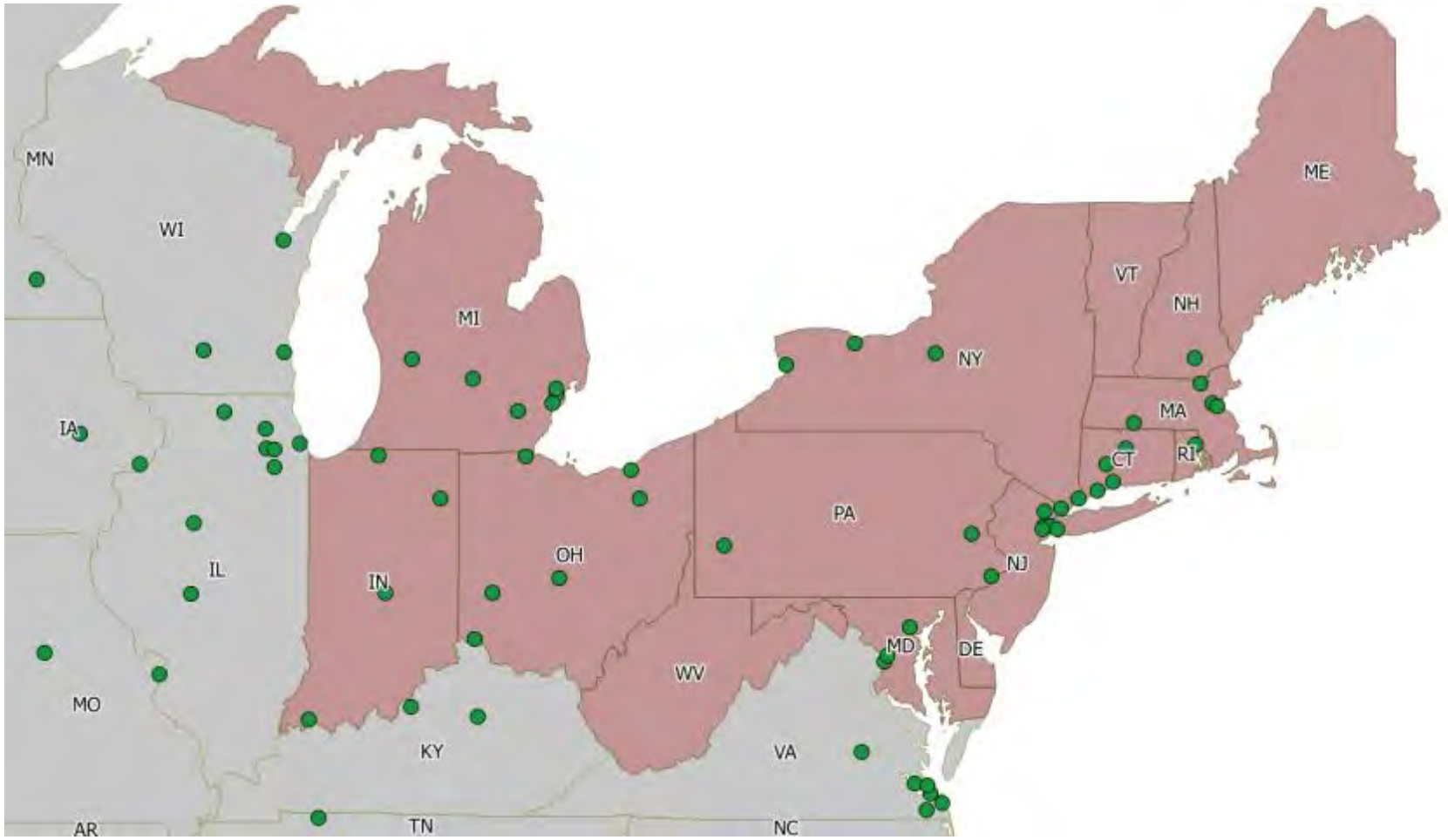
Day 3


MN
WI
MI
IA
IL
IN
OH
MO
KY
WV
VA
AR
TN
NC
PA
NY
ME
VT
NH
MA
CT
RI
NJ
MD
DE

Day 7


MN
WI
MI
IA
IL
IN
OH
MO
KY
WV
VA
AR
TN
NC
PA
NY
ME
VT
NH
MA
CT
RI
NJ
MD
DE

Day 14


MN
WI
MI
IA
IL
IN
OH
MO
KY
WV
VA
AR
TN
NC
PA
NY
MD
DE
NJ
CT
RI
MA
VT
NH
ME

Macroeconomic Impact

- Uses Oxford Economics Macroeconomic Model of US Economy and Value of Lost Load (VOLL) estimation
  - Outage affects consumption, labour, exports, confidence, and other parameters
- 21% loss of output for 32% of economy for 1 month for current national GDP of $18 Trillion is around $100 Bn (0.6%)
- However this shock cascades across the broader economy and effects continue to be felt for up to three years
  - It also affects the economies of other countries that trade with US
- GDP@Risk: US GDP reduces by: **$243 Bn**
  - Lost output resulting from incapacity of economic activity in region
  - 0.5% of US economy over 3 years

Insurance Industry Impact

Insurance payouts will be affected by

- Coverage
  - affirmative
  - silent
- Exclusions
- Deductibles
- Limits
- Legal judgements

Insurance Policy Analysis

- FirstEnergy's W. H. Sammis Power Plant is largest coal-fired power plant in Ohio
- 7 coal-fired generators and 5 oil-fired generators produce 2,233 megawatts.
- Policy details:
  - Annual Premium
  - Total Insured Values Buildings, Contents, Business Interruption
  - Limits
  - Deductibles
  - Exclusion Clauses

Coincidentally the loss of FE's Sammis-Star 345 kV line triggered the uncontrollable cascade portion of the 2003 blackout sequence.

Insurance Claimants

- Power generation companies
  - Property damage to their generators
  - Business interruption from being unable to sell electricity
  - Incident response costs and fines from regulators for failing to provide power
- Defendant companies
  - Companies sued by power generation businesses to recover some of their losses under defendants' liability insurance
- Companies that lose power
  - Property losses (principally to perishable cold store contents)
  - Business interruption from power loss (with suppliers' extension)
  - Failure to protect workforces or causing pollution as a result of the loss of power
- Companies indirectly affected
  - Contingent business interruption and critical vendor coverage
  - Share price devaluation generates claims under their directors' and officers' liability insurance
- Homeowners
  - Property damage, principally resulting from fridge and freezer contents defrosting,

Insurance Industry Impact

- It is identified as a cyber attack but never attributed to a perpetrator
- It is not formally declared as a terrorist act, or recognised as an official act of war
- The total of claims paid by the insurance industry is estimated at $21.4 billion

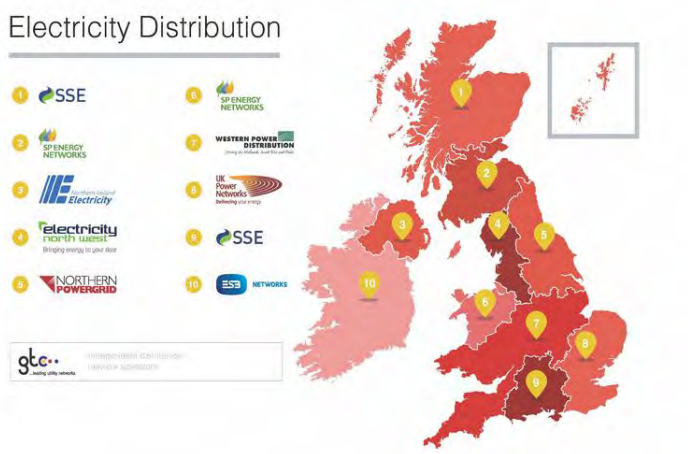
Erebos Blackout Scenario Launch Events

- 8th July 2015 – Lloyd's report on *The insurance implications of a cyber attack on the US power grid*
  - Report available from Lloyd's website
  - Results from research carried out by Centre for Risk Studies
- Centre for Risk Studies London Risk Briefings
  - *Cyber Risk in Operational Technology*, September date TBD

LLOYD'S

UK Critical Infrastructure Cyber Threat Stress Test Scenario

- UK Power Outage
- Impact on Critical National Infrastructure
- Secondary Shocks
- Stakeholder Interviews
  - UK Power Industry
  - UK Government
- Scenario Development Workshop
  - Cabinet Office
  - DECC
  - CPNI
  - GCHQ
  - UK Power Industry
  - UK/European Insurance Industry
  - Cyber security experts



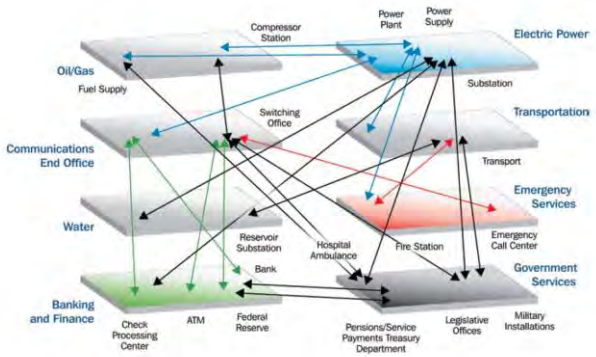


FIGURE 3.1 Connections and interdependencies across the economy. Schematic showing the interconnected infrastructures and their qualitative dependencies and interdependencies. SOURCE: Department of Homeland Security, National Infrastructure Protection Plan, available at http://www.dhs.gov/xprevprot/programs/editorial_0827.shtm.

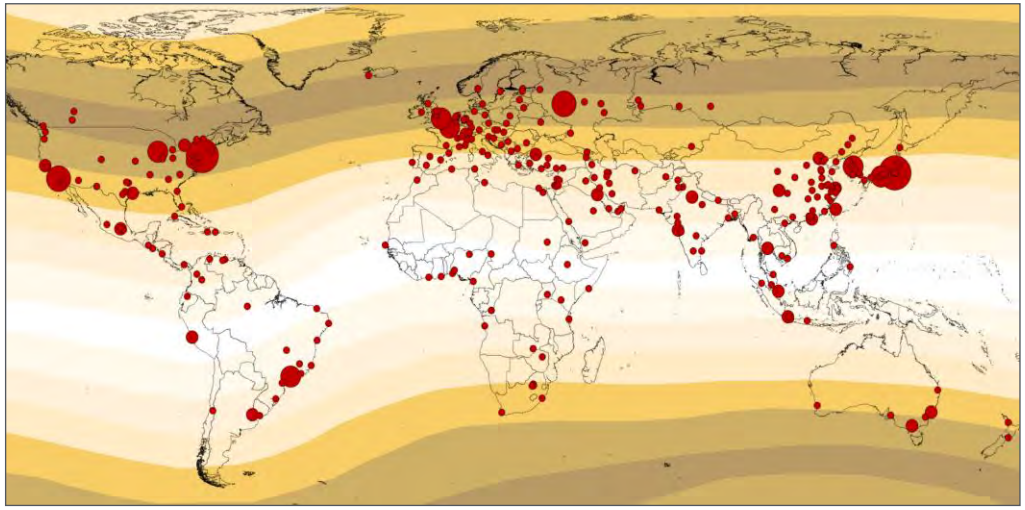
The Need for a Standardised Cyber EDM

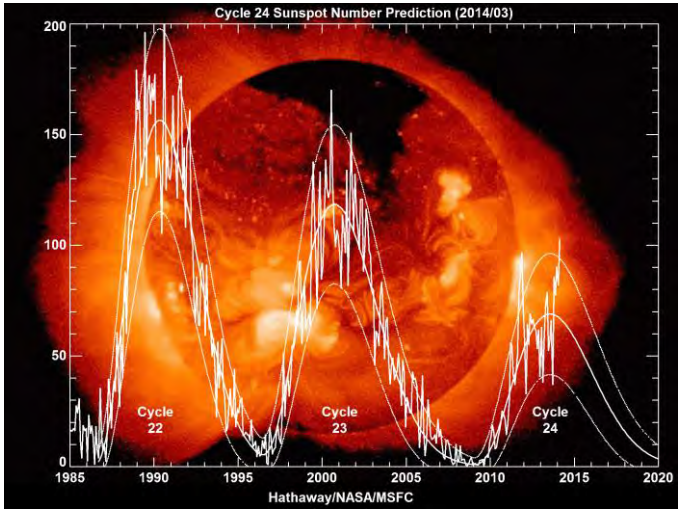
- The insurance industry manages its exposure data in a wide variety of ways
- Cyber is a new class of exposure
- Today many insurers have improvised their own method of capturing their cyber exposure data – every one is different
  - To date we have spoken to over 35 insurance companies
- Standardisation of cyber exposure data is generally perceived to be desirable and would benefit:
  - Exchange of information between companies
  - Reinsurance risk transfer
  - Regulators
  - Models of risk
  - Accumulation management
- The standardisation of a cyber EDM is necessary for development of a proper market for cyber insurance

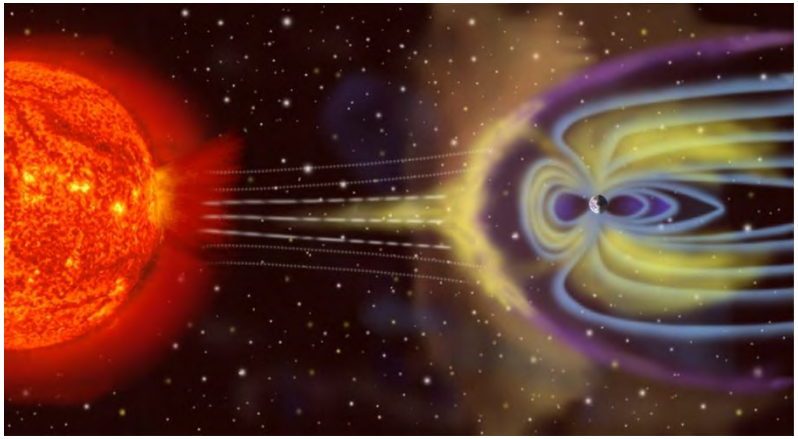
Cyber EDM Data Schema

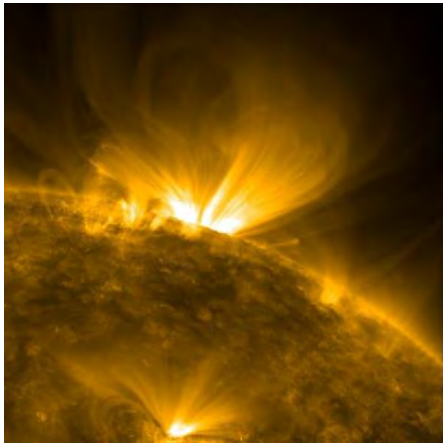
- Affirmative Cyber Products
  - Standardized coverage
- Affirmative Cyber Coverage
  - Advanced/bespoke coverage
- Silent Cyber Coverage
  - 'All Risks' policies without explicit exclusions

‘Helios’ Solar Storm Stress Test Scenario









Cyber Research at the Centre for Risk Studies

- Highly applied
- Plays active role in industry
- Provides tools to help risk management process
- Helps three stakeholder groups
  - Insurance
  - Corporate Sector
  - Government

Centre for
Risk Studies

UNIVERSITY OF
CAMBRIDGE
Judge Business School