Integrated Infrastructure:
Cyber Resiliency in Society

Centre for
Risk Studies

UNIVERSITY OF
CAMBRIDGE
Judge Business School

LOCKHEED MARTIN

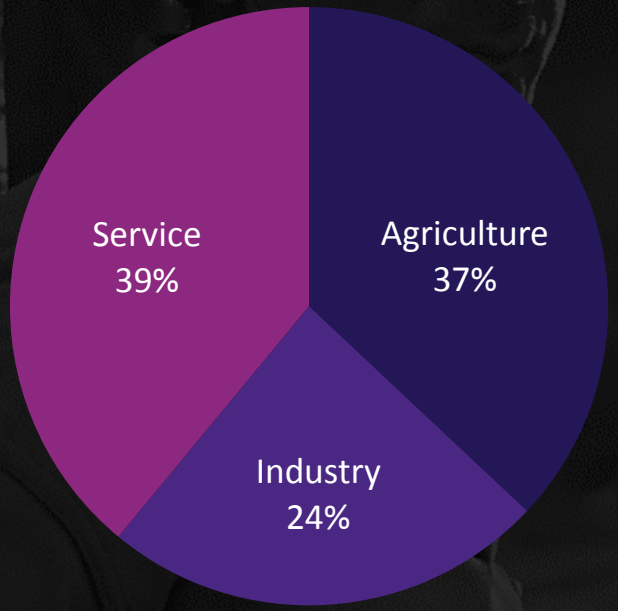
The Knowledge Economy

OLD

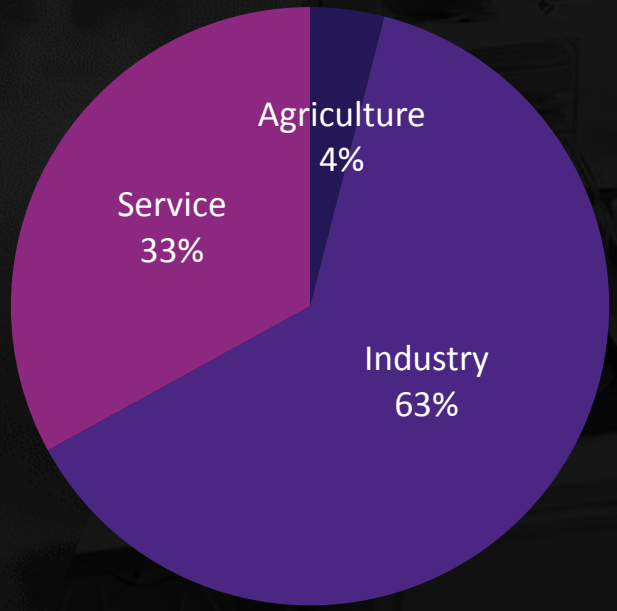
Economies categorised by dependency on critical infrastructure

NEW

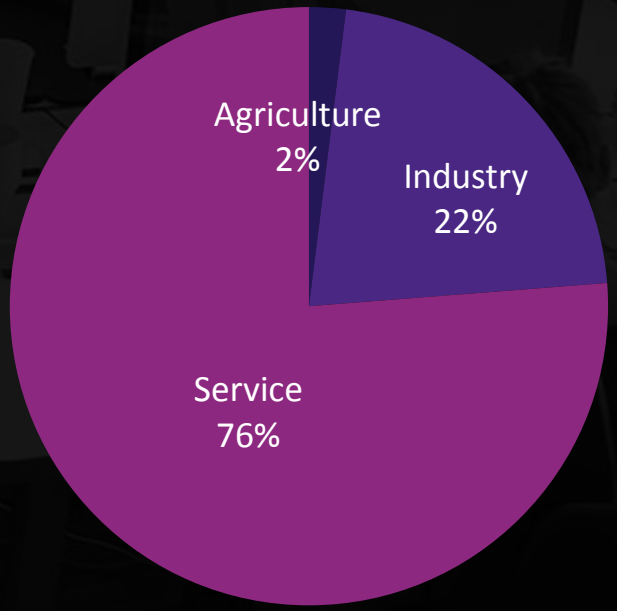
Agriculture with Industry & Service



Service-Dominated Economy

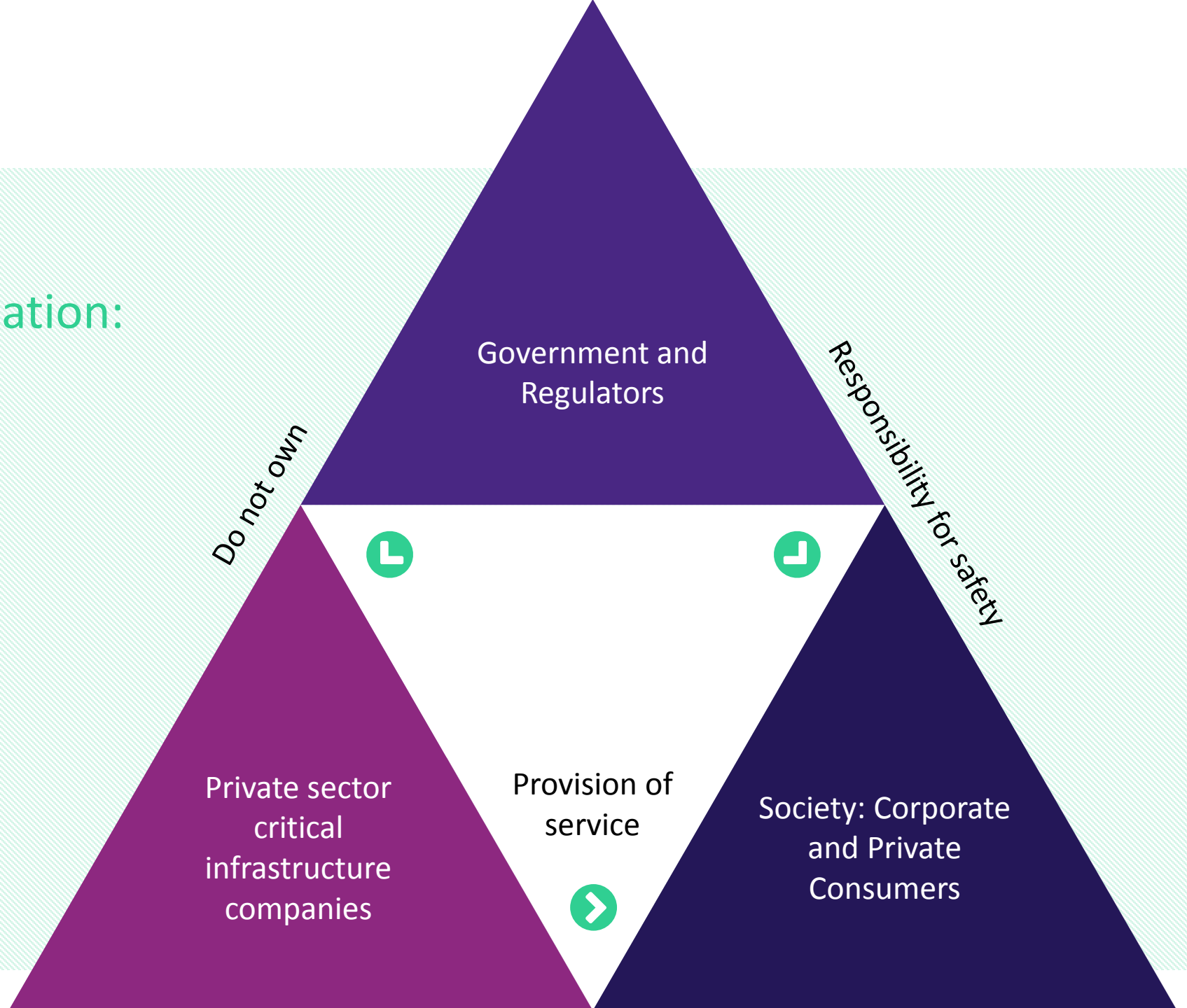


Service-Dominated Economy



Triangle of Pain

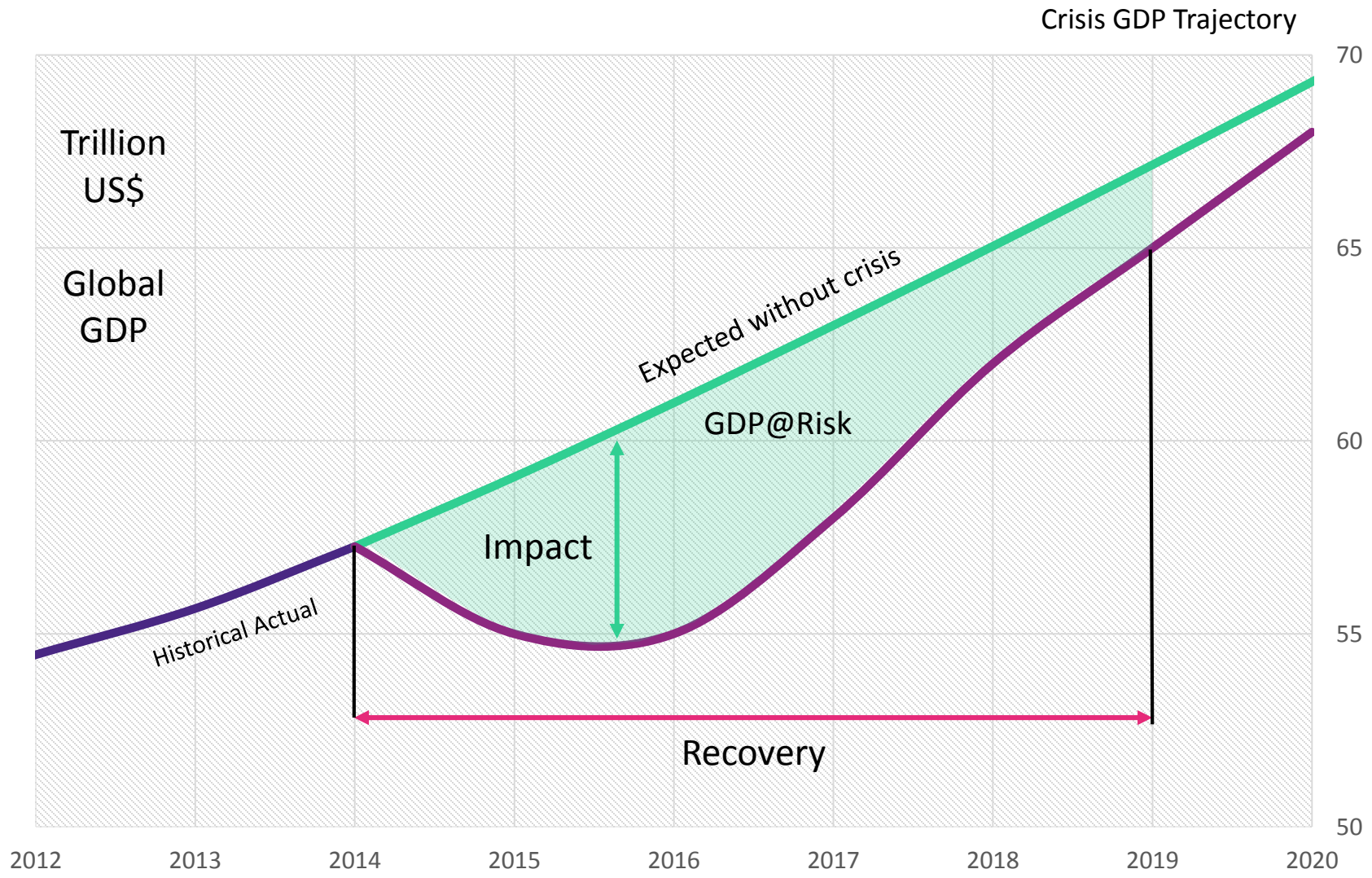
Optimizing the Risk Equation: Who Bears the Risk?



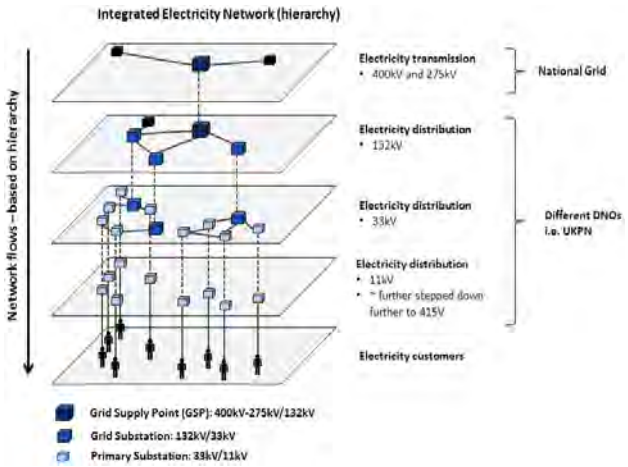
Catastronomics: GDP@Risk

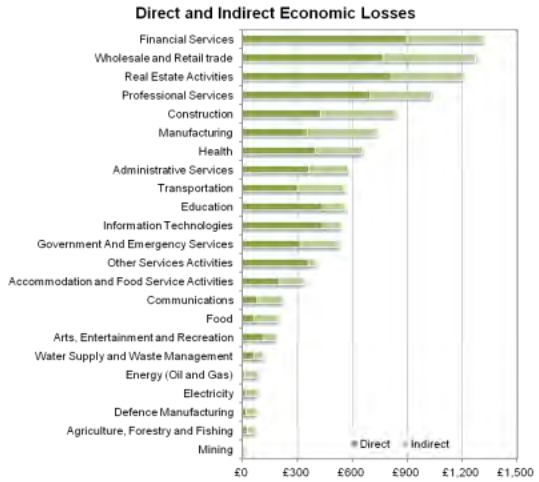
GDP@Risk:

Cumulative first five year loss of global GDP, relative to expected, resulting from a catastrophe or crisis



Methodology





Disruption to UK Society: Through risk and vulnerability modelling, using a system-of-systems model

Company & Supply Chain impact: Through supply-side input-output modelling

Impact on the UK Economy: Through macroeconomic modelling

The Cyber Scenario

Eireann Leverett

Ukraine Cyber Attack

- Date of power outage: 23 December 2015
- Electricity outage affected region with over 200,000 people for several hours
- Malware (BlackEnergy) in 3 distribution substations
- Still investigating if switching came from hackers
  - The Ukrainian energy ministry probing a “suspected” cyber attack on the power grid
- Ukraine CERT confirms there was spear phishing at affected companies prior to outage

ft.com > companies >

You are signed in

Search for...

Technology

Home UK World Companies Markets Global Economy Lex Comment Management Personal Finance Life & Arts

Energy Financials Health Industrials Luxury 360 Media Retail & Consumer Tech Telecoms Transport By Region Tools

Click here to try **our new website** — you can come back at any time

Last updated: January 5, 2016 10:37 pm

Hackers shut down Ukraine power grid

Hannah Kuchler in San Francisco and Neil Buckley in London

Share Author alerts Print Clip Gift Article Comments

Hackers brought down the power supply to hundreds of homes in Ukraine last week, in a cyber attack believed to be the first ever to result in a power outage.

The Ukrainian energy ministry said it was probing a “suspected” cyber attack on the power grid, targeting several regional power companies, which the country’s intelligence service blamed on “Russian special services”. Moscow has not responded to the allegation.

EMAIL BRIEFING

Sign up to #techFT, the FT’s daily briefing on tech, media and telecoms.

Sign up now

NEWS BY EMAIL

Sign up for email briefings to stay up to date on topics you are interested in

MOST POPULAR Read Commented Videos

1. Brent crude oil slides below $35 for first time since

Kuchler Hannah and Neil Buckley. “Hackers shut down Ukraine power grid.” Financial Times. 5 January 2016. http://www.ft.com/cms/s/0/0cfffe1e-b3cd-11e5-8358-9a82b43f6b2f.html#axzz3wTmkfdX9 [Accessed: 6 Jan 2016]

Standard Disclaimer

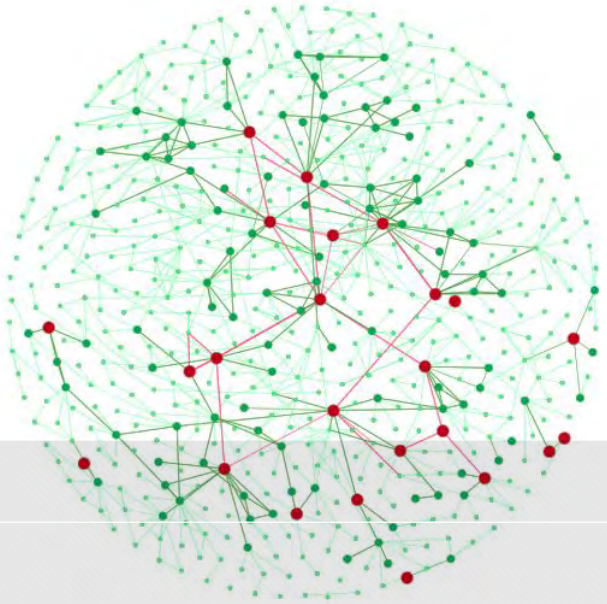
This scenario is not a prediction

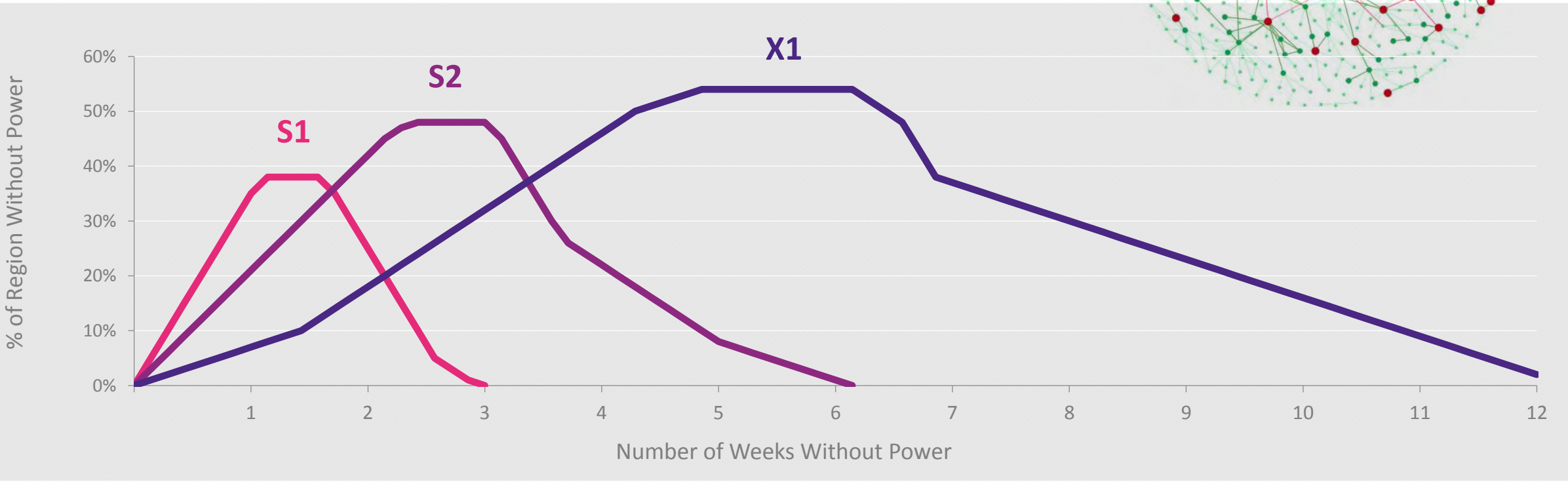
It is not trying to highlight any specific vulnerability in the UK Power Grid

This is a stress test scenario for risk management purposes

The Scenario

- Attack on electricity distribution in South East England
- Key focus on 132kV distribution substations
- Insider + State Sponsored Cyber Team
- Rogue hardware attack platform installed inside substation
- Rolling blackouts





{ Phase 1 }

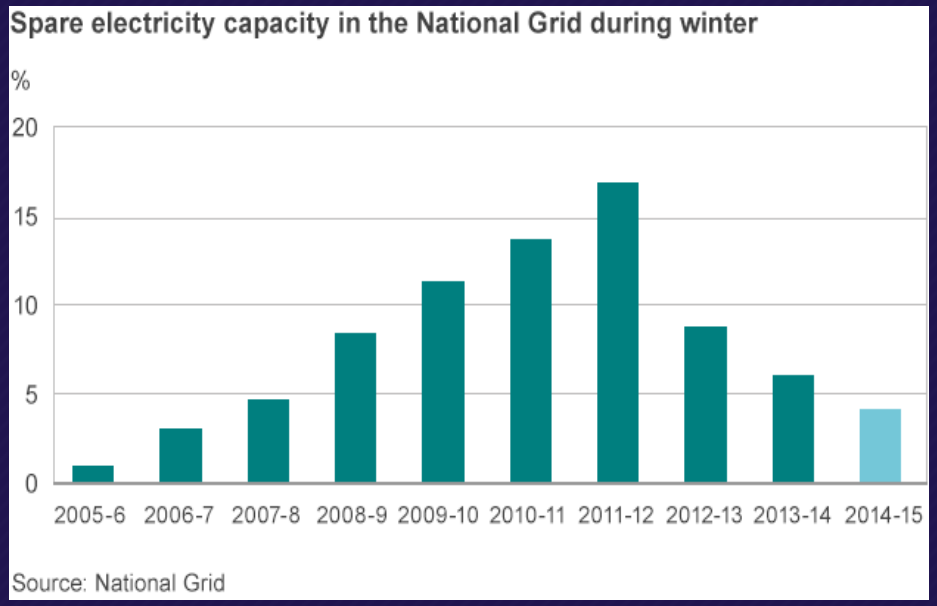
Research and Development

- Nation State + Insider
- Sub-contract Employee
- Installs rogue PLC Hardware
- 1-5 substations installed per week over 6 months
- Minimum 65 substations affected

{ Phase 1 }
Research and Development

Target Location and Timing

- With inside support, the nation is able to target critical substations
  - Heathrow (X1 only), Gatwick, Stansted and City Airports
  - London Financial District
  - Ports of London and Dover
  - Felixstowe Container Port
- The attack begins during a cold period during winter when electricity demand is at its highest
  - During the 2015/16 winter season it is predicted that on the highest demand day (i.e., the coldest day) there will only be a 5.1% capacity margin, meaning that there is little room for error



BBC. “National Grid warns of lower winter power capacity”. 28 October 2014.

{ Phase 1 }
Research and Development

Rogue Hardware Attack Platforms: PLC PWN

Malicious Hardware

It is difficult to identify rogue hardware

Hilt, S. (2014, February 3). PLCpwn. Retrieved July 22, 2015, from Digital Bond: http://www.digitalbond.com/blog/2014/02/03/s4x14-videostephen-hilt-on-plcpwn/

{ Phase 1 }
Research and Development

- Nation State + Insider
- Sub-contract Employee
- Installs rogue PLC Hardware
- 1-5 substations installed per week over 6 months
- Minimum 65 substations affected

{ Phase 2 }
Deployment and Dormancy

- Rogue Hardware Communication via 3/4G
- Attacks require physical presence to fix
- Attackers spend time mapping substation networks
- Supported by a set of ‘cover attacks’

{ Phase 1 }
Research and Development

- Nation State + Insider
- Sub-contract Employee
- Installs rogue PLC Hardware
- 1-5 substations installed per week over 6 months
- Minimum 65 substations affected

{ Phase 2 }
Deployment and Dormancy

- Rogue Hardware Communication via 3/4G
- Attacks require physical presence to fix
- Attackers spend time mapping substation networks
- Supported by a set of 'cover attacks'

{ Phase 3 }
Activation

- 10 substations attacked every 12 hours

<u>Days 1-2:</u>

- Control signals spoofed
- DNO unaware until customers report
- Once cyber attack suspected, control centre investigation starts
- Defence response occurs on 2nd or 3rd outage

<u>Days 1-2:</u>

- Engineer electrocuted
- Rogue hardware still unidentified
- Investigation moves to substations

{ Phase 1 }
Research and Development

- Nation State + Insider
- Sub-contract Employee
- Installs rogue PLC Hardware
- 1-5 substations installed per week over 6 months
- Minimum 65 substations affected

{ Phase 2 }
Deployment and Dormancy

- Rogue Hardware Communication via 3/4G
- Attacks require physical presence to fix
- Attackers spend time mapping substation networks
- Supported by a set of 'cover attacks'

{ Phase 3 }
Activation

- 10 substations attacked every 12 hours

Days 1-2:

- Control signals spoofed
- DNO unaware until customers report
- Once cyber attack suspected, control centre investigation starts
- Defence response occurs on 2nd or 3rd outage

Days 1-2:

- Engineer electrocuted
- Rogue hardware still unidentified
- Investigation moves to substations

{ Phase 4 }
The Response

Days 7- 14:

- Continued rolling blackouts
- Cabinet Office & CPNI confirm cyber attack
- Intelligence & security services involved
- Cover attacks confuse response
- Rogue PLC discovered after 1 week

Days 14 – 21

- Rogue device removal in progress
- Outages continue
- Physical damage to transformers

Physical Damage to Transformers

- In the X1 scenario variant, physical damage occurs via to the cyber attack to the transformers
- Transformers are naturally prone to overheating and thus have built-in cooling systems and di-electric mediums to prevent arcing
- Additionally, each transformer that fails increases the load on the power grid causing instability and, potentially, a cascading power failure

Literature on transformer damage includes

- Fire and Explosions in Substations (Allan, Fellow, IEEE, 2002),
- Using Hybrid Attack Graphs to Model Cyber Physical Attacks in the Smart Grid (Hawrylak et al, IEEE, 2012),
- A Coordinated Multi-Switch Attack for Cascading Failures in Smart Grid (Liu et al, IEEE, 2014),
- The Potential For Malicious Control In A Competitive Power Systems Environment (DeMarco et al, IEEE, 1996),
- Modelling Cyber-Physical Vulnerability of the Smart Grid With Incomplete Information (Srivastava et al, 2013)

{ Phase 1 }
Research and Development

- Nation State + Insider
- Sub-contract Employee
- Installs rogue PLC Hardware
- 1-5 substations installed per week over 6 months
- Minimum 65 substations affected

{ Phase 2 }
Deployment and Dormancy

- Rogue Hardware Communication via 3/4G
- Attacks require physical presence to fix
- Attackers spend time mapping substation networks
- Supported by a set of 'cover attacks'

{ Phase 3 }
Activation

- 10 substations attacked every 12 hours

Days 1-2:

- Control signals spoofed
- DNO unaware until customers report
- Once cyber attack suspected, control centre investigation starts
- Defence response occurs on 2nd or 3rd outage

Days 1-2:

- Engineer electrocuted
- Rogue hardware still unidentified
- Investigation moves to substations

{ Phase 4 }
The Response

Days 7- 14:

- Continued rolling blackouts
- Cabinet Office & CPNI confirm cyber attack
- Intelligence & security services involved
- Cover attacks confuse response
- Rogue PLC discovered after 1 week

Days 14 – 21

- Rogue device removal in progress
- Outages continue
- Physical damage to transformers

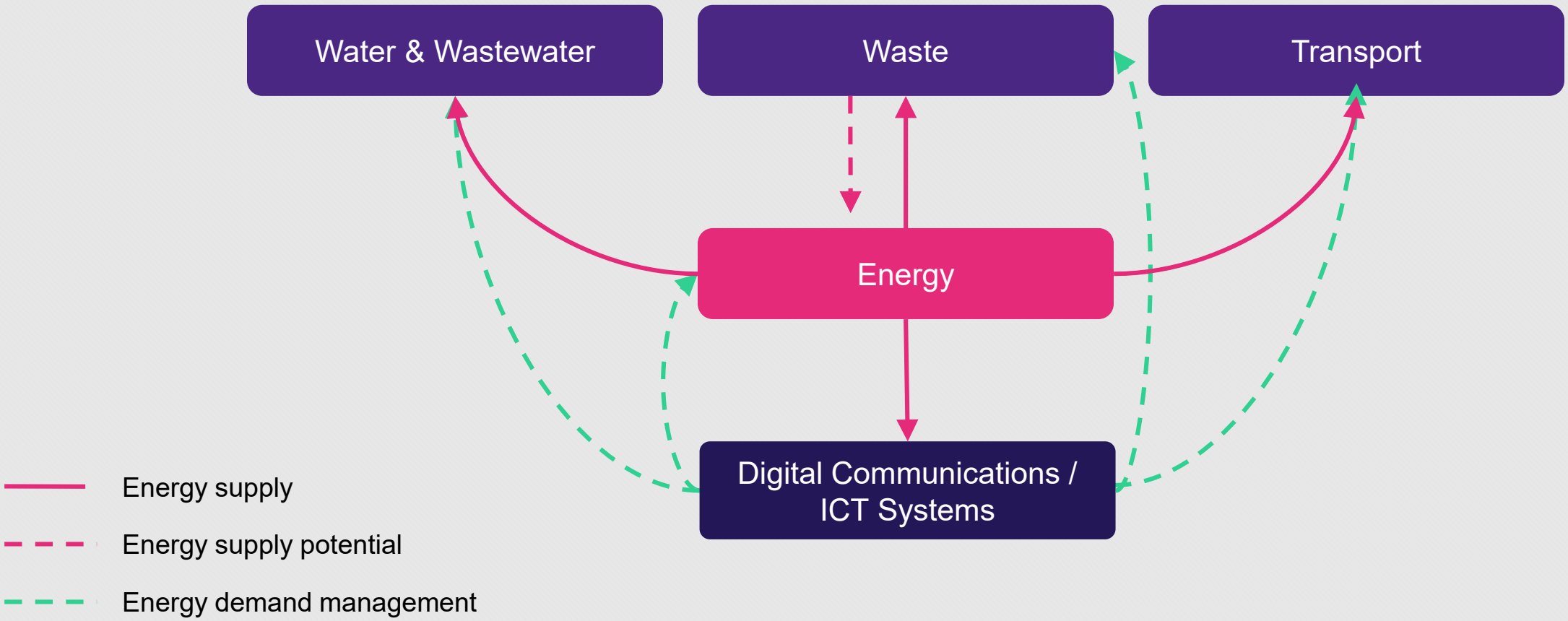
{ Phase 5 }
The Aftermath

- Vulnerabilities addressed and repairs complete within 1 year
- Perpetrators never positively identified
- Series of independent commissions investigate
- Public confidence weakened
- UK critical infrastructure impacted overtaken by nearby competitors
- Cyber security budgets increase
- Potential increase in energy costs with increased physical & cyber security spend

Economic Impact

Dr. Edward Oughton

Growing Interdependency: How to Quantify?

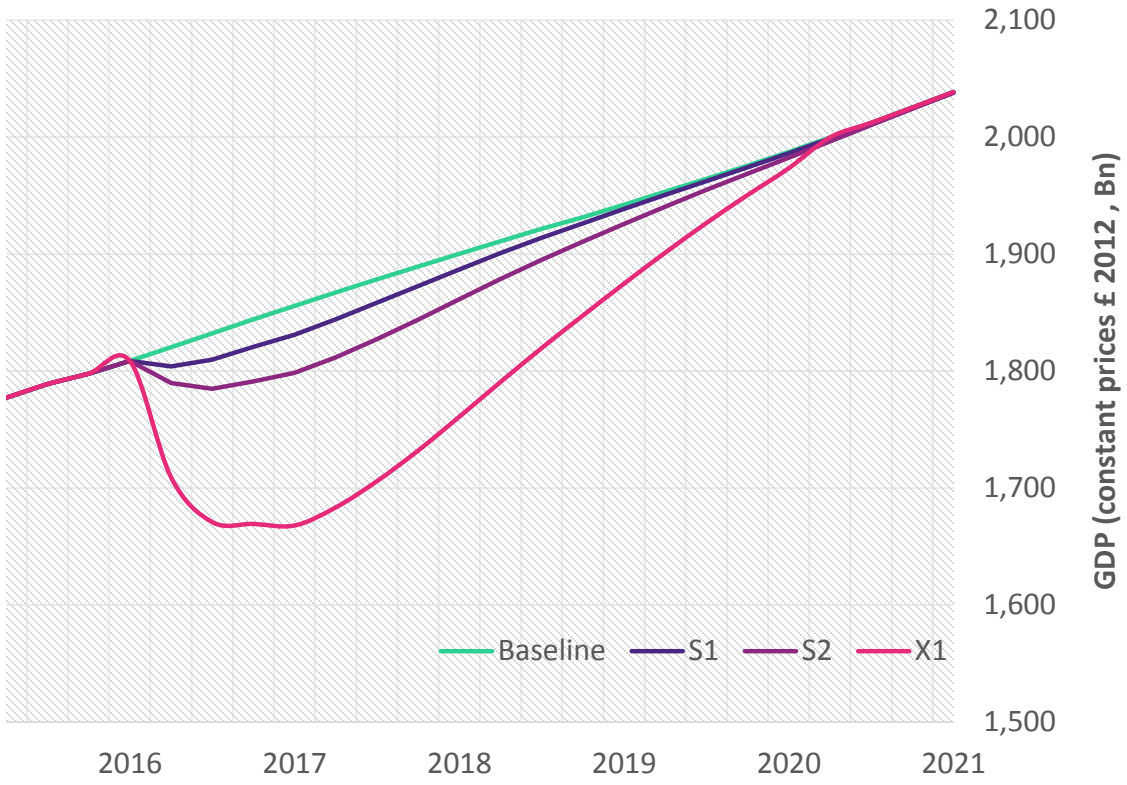


Summary of Scenario Variants

Scenario Variant	Description of Outage	Number of substations compromised with rogue hardware	Length of cyber attack campaign (weeks)	Effective total length of power outage (weeks)	Time to identify first rogue device in one substation (weeks)	Period for reverse engineering and planning the clean-up (weeks)	Clean-up and power recovery period (weeks)	DNO region(s)	Physical Damage
S1	Optimistic/Rapid Response	65	3	1.5	1	1	1	1 region	No
S2	Conservative/Average Response	95	6	3	1	2	3	1 region	No
X1	Extreme/Average response + physical transformer damage + 2 rogue devices + 2 regions	125	12	6	2	4	6	>1 region	Yes

Modelled Results

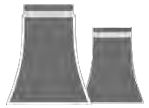
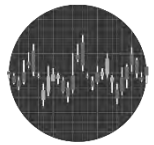
Scenario Variants	Lost power (TWh)	Production (1 year direct) Sector Losses £ billion	Supply Chain (1 year indirect) Sector Losses £ billion	GDP@Risk (5 Yr) impact on overall UK economy £ billion
S1	10.3	7.2	4.4	49
S2	19.8	18.0	10.9	129
X1	39.6	53.6	31.8	442



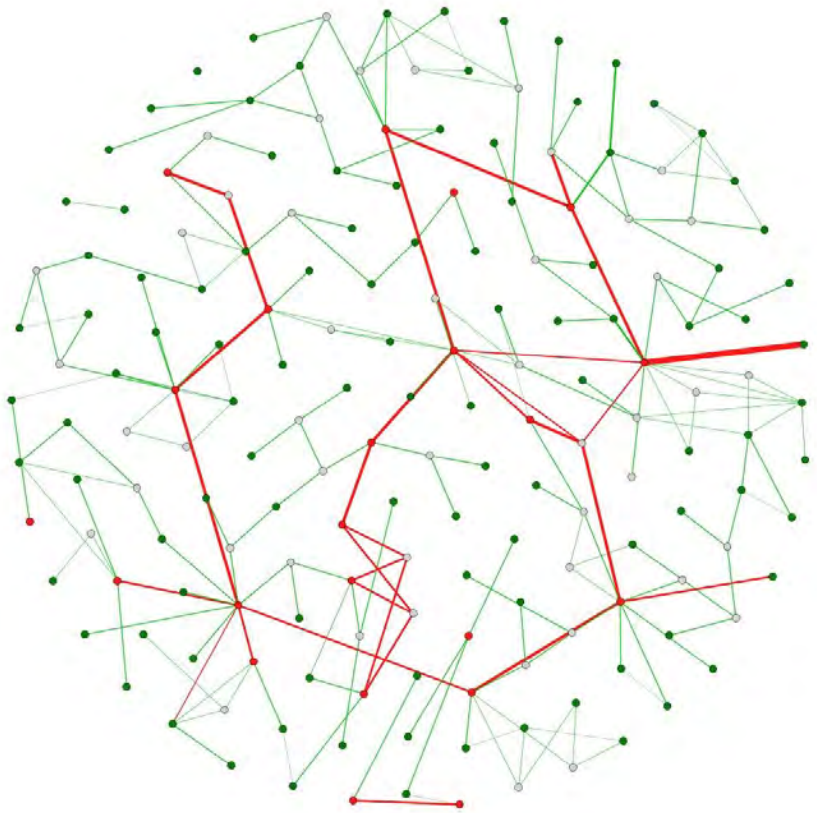
Domestic UK GDP@Risk under each scenario variant

£ billion

Highlights

 **9 m**	▪ Electricity customers disrupted ▪ Similar levels of disruption experienced across other critical infrastructure sectors
 **£7 BN**	▪ Direct industrial production losses
 **£4 BN**	▪ Indirect supply chain losses
	▪ Worst affected critical infrastructure sector: Financial services
	▪ Worst affected economic sector: Wholesale and Retail Trade
 **£49 BN**	▪ 5-year GDP@Risk

Conclusions



- Cooperation and transparency needed across sectors:
  - This isn’t a power generation/distribution problem
  - No-one talking about how it all fits together - don’t think in silos
- OT and IT to share experience and knowledge – OT to improve resilience, ensure separation/protection of respective infrastructures
- People still don't believe these scenarios can happen, evidence shows otherwise
- As a largely service & knowledge based economy the impacts for the UK immediate in key sectors
- Government has a key role in coordination and prioritisation

Panel Q&A Session

Centre for
Risk Studies

UNIVERSITY OF
CAMBRIDGE
Judge Business School

LOCKHEED MARTIN

Integrated Infrastructure:
Cyber Resiliency in Society

For more, visit lockheedmartin.com/blackout

Centre for
Risk Studies

UNIVERSITY OF
CAMBRIDGE
Judge Business School

LOCKHEED MARTIN