CITY UNIVERSITY LONDON

Evaluating resilience of multiple infrastructures: some challenges

RACI, San Jose dos Campos, April 2011

Robin E Bloomfield
Adelard LLP and CSR City University London

reb@adelard.com
reb@csr.city.sc.uk
College Building, City University, London EC1V 0HB
Tel: +44 20 7490 9450 (sec Adelard)
Tel: +44 20 7040 8420 (sec CSR)

CSR Building confidence in a computerised world
www.csr.city.ac.uk

Adelard

Challenges

- The nature of “resilience” and a need for conceptual clarity
- The notion of “infrastructure” and the “system” and the need for a broader definition to address intangibles.
- The aims of risk assessment including risk communication, perception and transparency and different stakeholder viewpoints
- The practice of risk assessment including the need for data to support risk assessment, the importance of models and their use in extrapolation and the scale of epistemic uncertainties.
  - The importance of dependencies and interdependencies
- The immaturity of science and technology and our lack of knowledge of the role of different modelling approaches.
- The possible performative nature of the models.

CITY UNIVERSITY LONDON

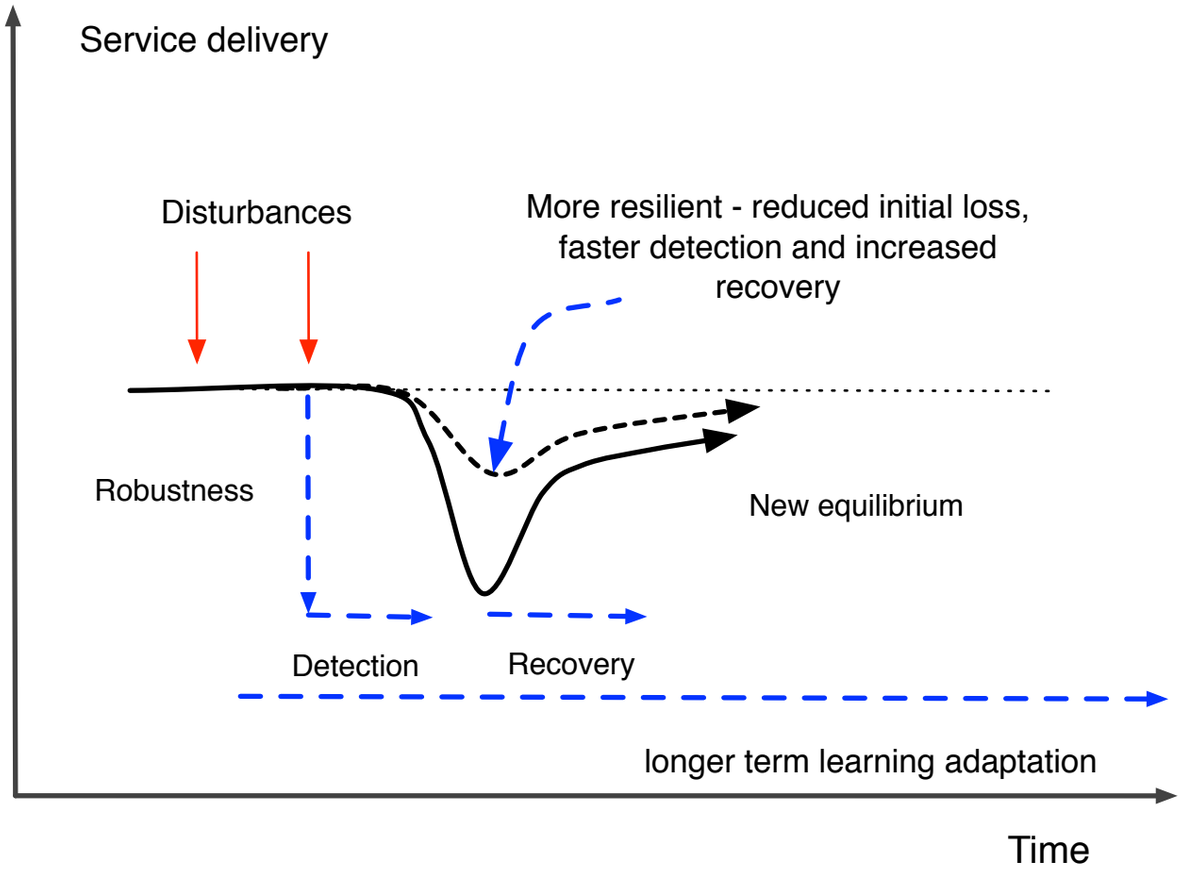
Resilience

Metaphors, models

CSR Building confidence in a computerised world
www.csr.city.ac.uk

Adelard

Concepts - resilience viewpoint



- *Type 1*: Resilience to design basis threats. This could be expressed in the usual terms of availability, robustness, etc. It could be bounded by credible worst case scenario.

- *Type 2*: Resilience to beyond design basis threats. This might be split into those known threats that are considered incredible or ignored for some reason and other threats that are unknowns.

- Attacks on intangibles - these are also societal assets, not just CIP

- Does addressing Type 2 help with Type 1?

Phase (see Figure 4)	Action to increase resilience
Preparation and learning	Reduce frequency of events by early warning and upstream measures Provide early warning, operator support Learning from experience (major incidents, minor mishaps, near misses), training
Initial loss	Increased robustness by • network design addressing topology, redundancy, diversity. Classification of critical nodes and suitable hardening. • understanding of events and scenarios
Detection	Communication between services Variety of forecasting approaches Detection of compromises
Decision	Situational awareness Planning and training (scenarios) and use of synthetic environments
Recovery	Resource deployment; dependent assets identified Awareness state of other networks Communication and co-ordination

Table 1: Phases of resilience

Different emphasis

- All hazards approach: all hazards are considered, including both natural disasters and malicious attacks.
  - Security and vulnerability focus: identification of security critical assets and consideration of vulnerabilities/threats to them.
  - Natural hazard focus: only considers events such as floods/earthquakes and their effect on infrastructure.

- And also the overall purpose of their analyses e.g.
  - Identification of vulnerabilities (dependencies) in stable system state
  - Incident response, i.e., control of the incident and evacuation and coordination of emergency services
  - Long-term effects and recovery e.g., environmental, financial

Resilience

- *Type 1*: Resilience to design basis threats. This could be expressed in the usual terms of availability, robustness, etc. It could be bounded by credible worst case scenario.
- *Type 2*: Resilience to beyond design basis threats. This might be split into those known threats that are considered incredible or ignored for some reason and other threats that are unknowns.

- Design basis
  - need to address both the endogenous/exogenous nature of the initiating events and the extent to which they are emergent system properties or addressable by more reductionist approaches.
- Note that complex infrastructure systems evolve
  - balance between design and evolution
  - address governance and incentives that shape evolution

Soft, intangible, infrastructures

- consultations (in Cetifs) highlighted the importance of “soft” infrastructures
- assets such as trust and privacy emergent properties - have a complex relationship to localised issues.
- need to take into account these essential yet softer aspects and their relationship to the more tangible aspects.
- soft aspects are just as much the target of security threats as the more obvious physical and cyber systems.
- in the past the soft infrastructure might have been separable from the more technical infrastructures
- trust relationships increasingly mediated by the information infrastructure: a trend that is likely to increase.

CITY UNIVERSITY LONDON

Interdependencies

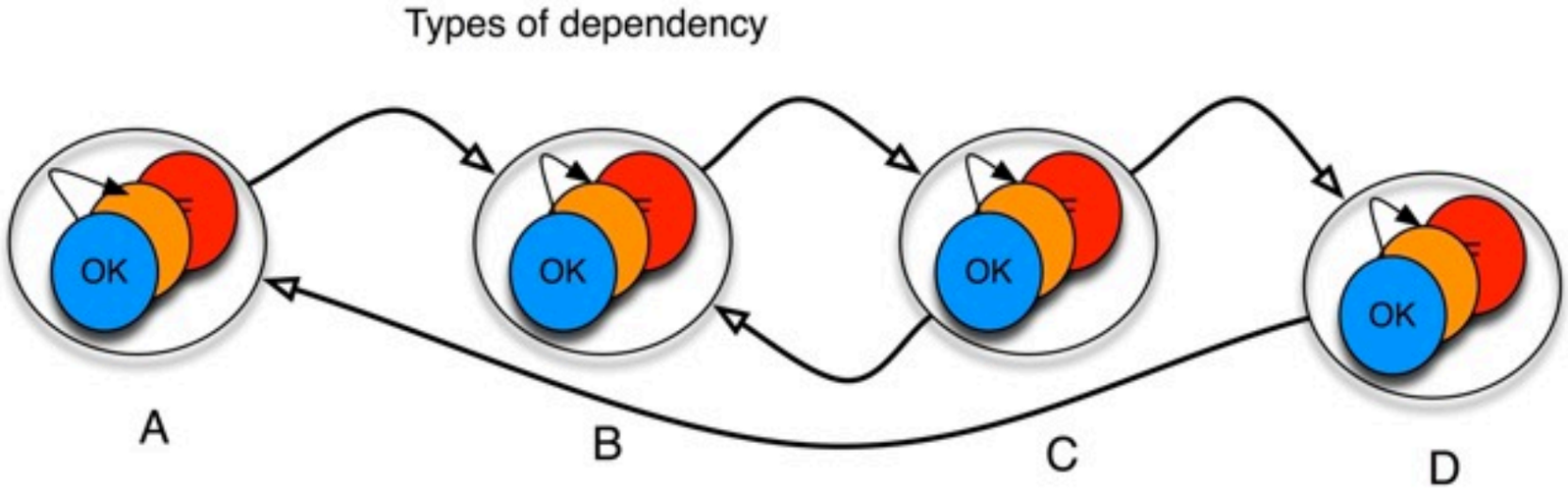
Metaphors, models, theories

CSR Building confidence in a computerised world
www.csr.city.ac.uk

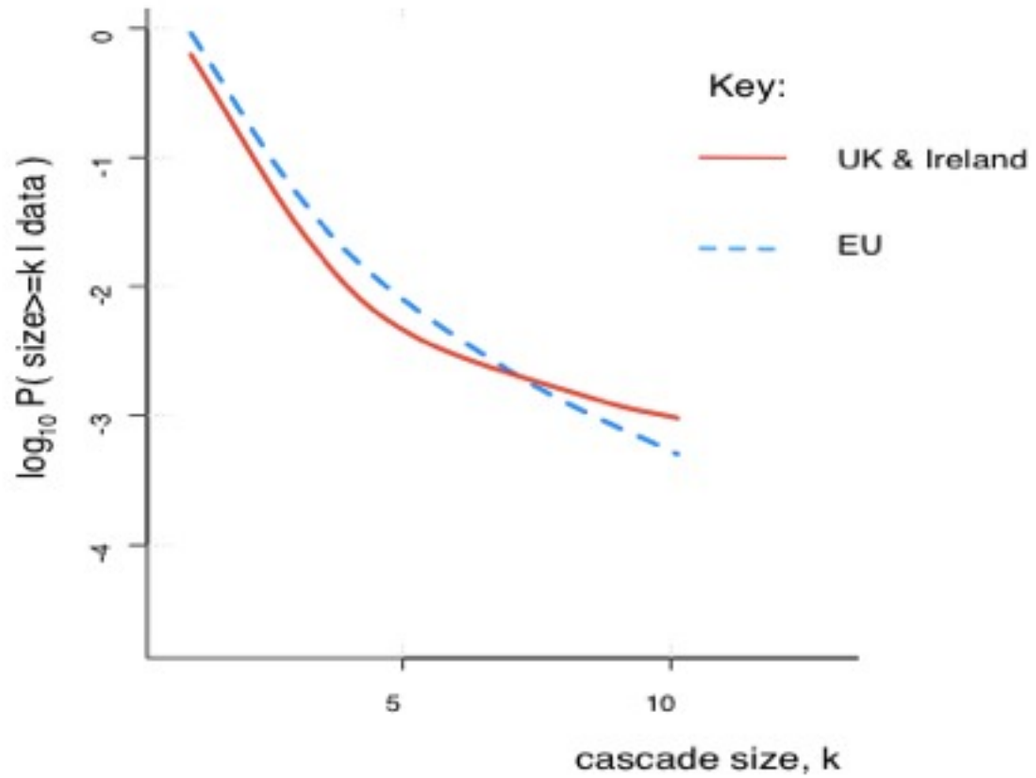
Adelard

Interdependencies

- Dependencies and interdependencies essential for achieving resilience but also a threat
  - Need connectivity (so implications for vulnerabilities)
  - Need resources to achieve resilience (so implications for optimality)



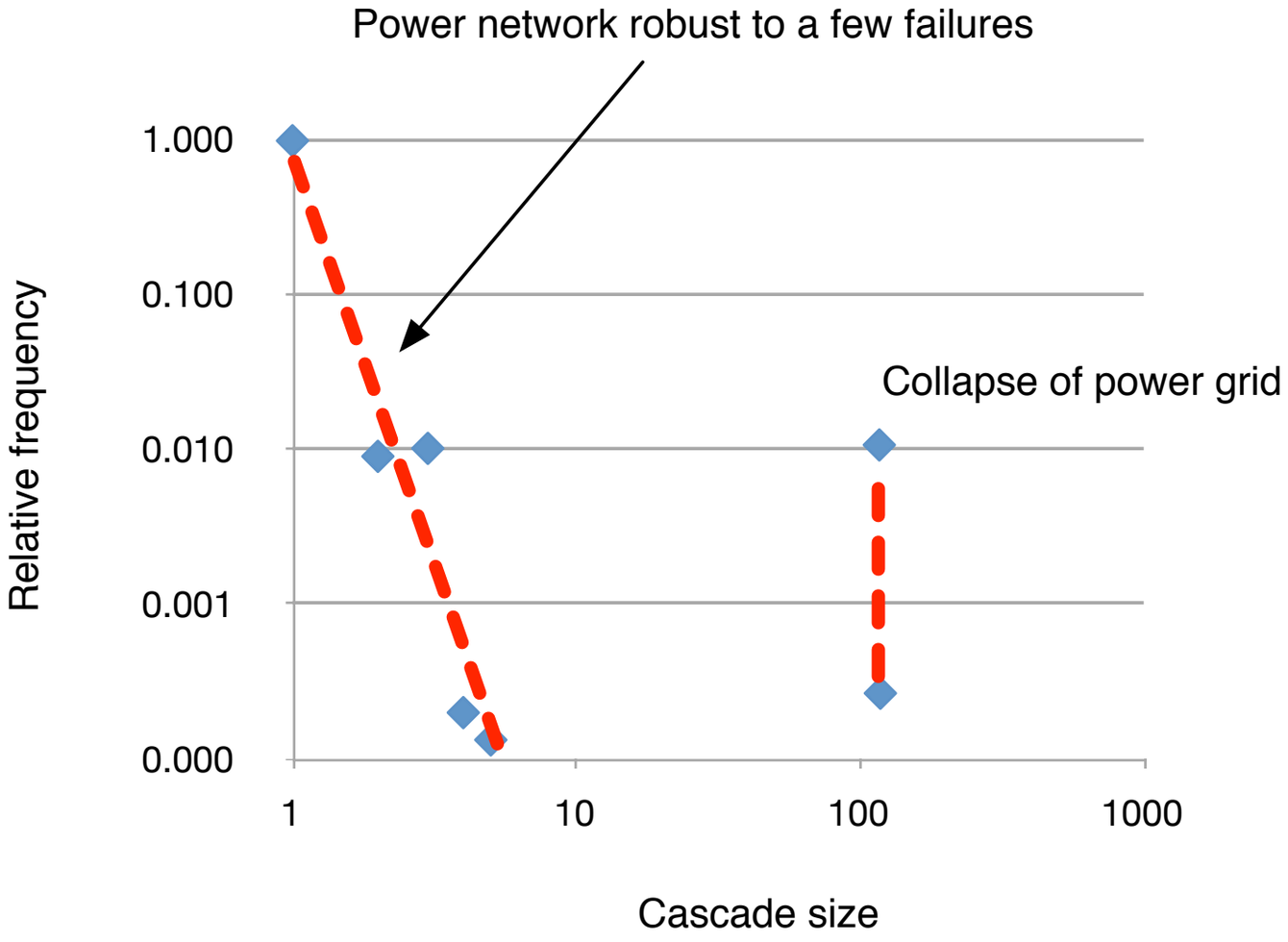
Empirical data - EU and UK



CSR Building confidence in a computerised world
www.csr.city.ac.uk

Adelard

Critical infrastructure

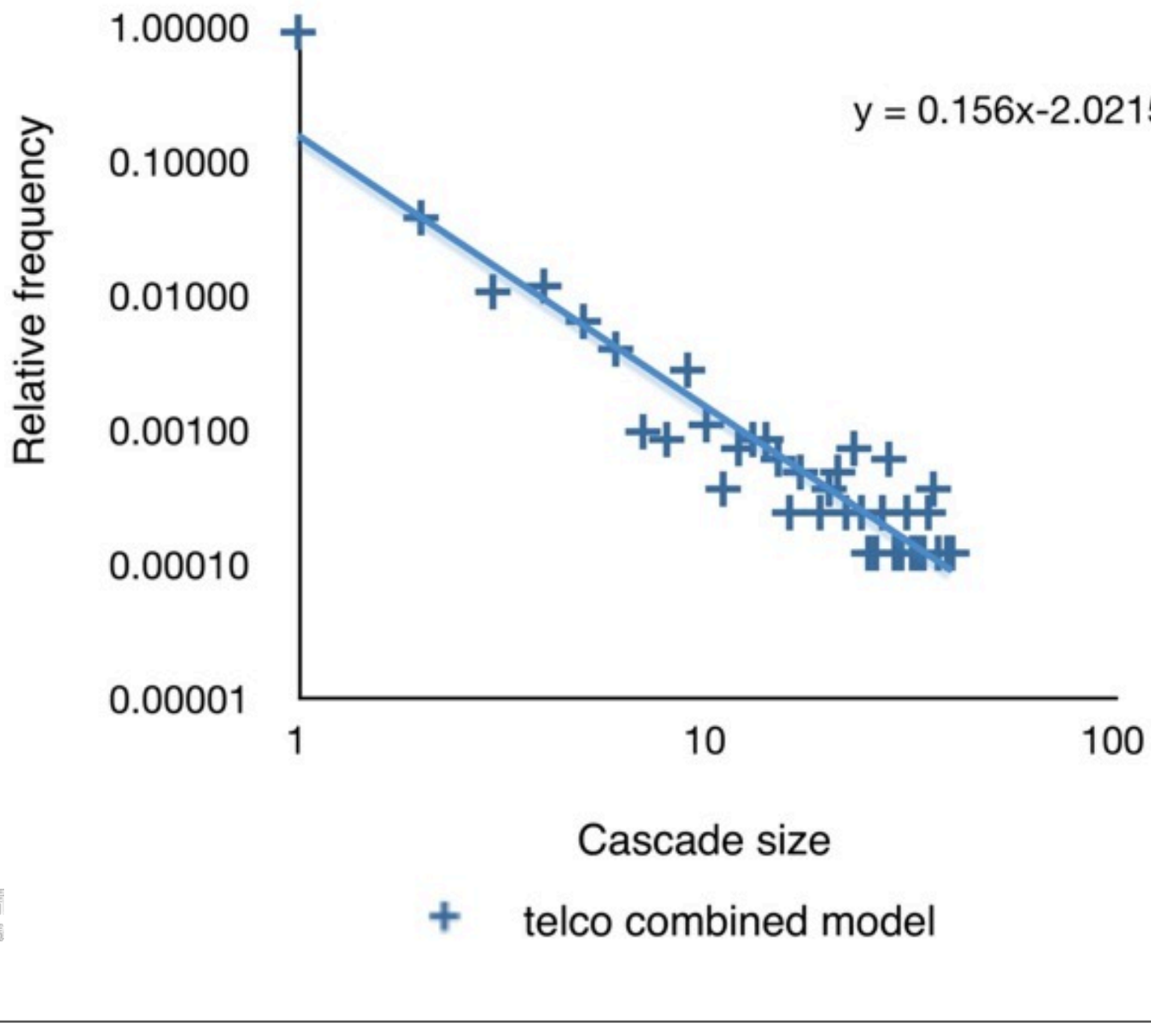


PIA FARA Rome Models

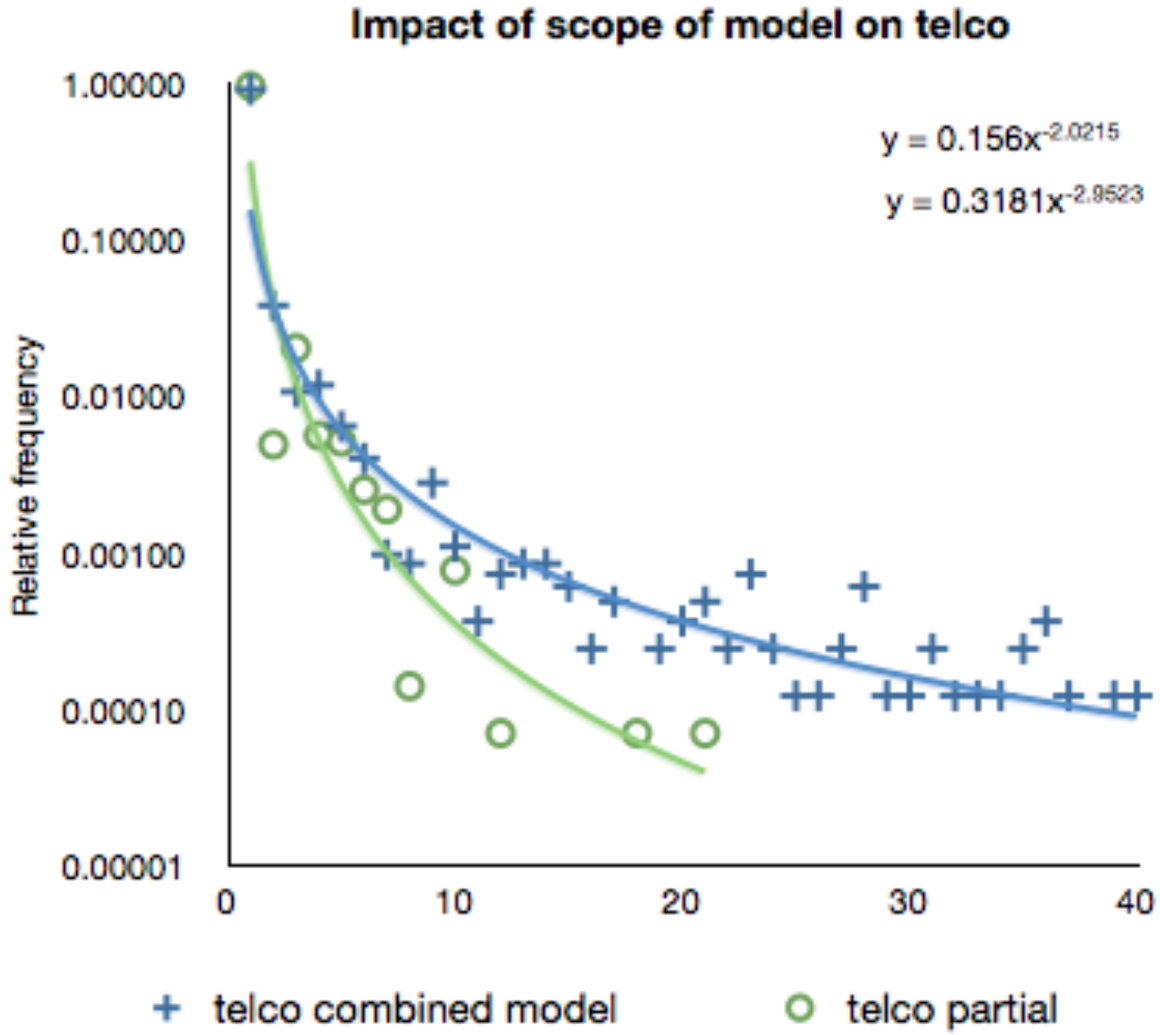
CSR Building confidence in a computerised world
www.csr.city.ac.uk

Adelard

Telco network



Impact of infrastructure interaction



CSR Building confidence in a computerised world
www.csr.city.ac.uk

Adelard

Performative models

- In the past, in the engineering domain, the models used to design and assess the risks do not affect the threats or challenges that the system faces
  - modelling severe weather does not change the wind speed in London
    - (except perhaps via a slow political process and peoples' behaviour)
  - in the financial area this is not the case: models can be what is termed *performative*, having a direct and unforeseen impact on the markets and how it fails
- engineered systems and security risks
  - knowledge and access to design models may inform an adversary and hence have a potential impact on the threats a system faces
  - *Donald MacKenzie , An Engine, Not a Camera: How Financial Models Shape Markets and also Do Economists Make Markets?: On the Performativity of Economics*

Conclusions

Challenges include:

- The nature of “resilience” and a need for conceptual clarity
- The notion of “infrastructure” and the “system” and the need for a broader definition to address intangibles.
- The aims of risk assessment including risk communication, perception and transparency and different stakeholder viewpoints
- The practice of risk assessment including the need for data to support risk assessment, the importance of models and their use in extrapolation and the scale of epistemic uncertainties.
- The immaturity of science and technology and our lack of knowledge of the role of different modelling approaches.
- The possible performative nature of the models.

CSR Building confidence in a computerised world
www.csr.city.ac.uk

Adelard