Infrastructure interdependency analysis:

Requirements, capabilities and strategy

Produced for CPNI, TSB and EPSRC, under contract NSIP/001/0001 –
Feasibility Study on Interdependency Analysis

CITY UNIVERSITY LONDON

Cranfield UNIVERSITY

Adelard

Authors

R Bloomfield, City University and Adelard LLP
N Chozos, Adelard LLP
P Nobles, Cranfield University

Document Control

Adelard document reference: **D/418/12101/3**

Executive summary

The Centre for the Protection of National Infrastructure (CPNI), the Technology Strategy Board (TSB) and the Engineering and Physical Sciences Research Council (EPSRC) have commissioned a feasibility study to identify the state-of-the-art in Critical Infrastructure (CI) interdependency modelling and analysis and to develop a strategy for research and practice, aiming to bridge the gaps between existing capabilities and Government/industry requirements.

The study, carried out by the Centre for Software Reliability of City University, Cranfield University, Defence Academy of the United Kingdom and Adelard LLP aims at assessing the technical and commercial feasibility of

- the development of tools and services for analysing interdependency between infrastructures, particularly information infrastructures, and assessing associated risks
- establishing "interdependency analysis" as a distinct and recognisable service supported by tools and data

The study is based on consultations with a wide a range of Critical National Infrastructure (CNI) stakeholders (government, industry and academia) and a review of research specific to modelling, analysing and overall understanding dependencies in infrastructures (in a separate report). The consultations and the research review have supported the third step of this study, which is a gap analysis that concludes to four potential capabilities that would address current requirements:

- To provide specialised security analysts with a means for the assessment of infrastructure interactions and interdependencies.
- To provide off line support for risk assessors—both aggregators of risk and also individual infrastructure owners to evaluate the impact of dependencies and interdependencies.
- To provide off line support for risk assessors—both aggregators of risk and also individual infrastructure owners during incidents (soft real-time).
- To provide real time, decision support integrated command and control systems (hard real-time).

In conclusion, the study proposes a strategy aiming at achieving the capabilities that were identified as currently feasible. The strategy consists of the following activities:

- *Trial state-of-the-art and emerging research.* Develop and trial modelling approaches and decision-support tools and methodologies at various levels of detail. Consider both qualitative approaches and off-line or real-time infrastructure interactions.
- *Provide policy support and evidence base.* Provide justification and focus of the programme, emphasising the benefits and responsibilities for all stakeholders. Develop effective business models.
- *Offer knowledge transfer and coordination.* Promote the research base and offer connection to practice by enabling interaction (e.g. via knowledge transfer activities), addressing costs of research and methodologies and developing a challenging research agenda.

Within each of these threads both natural hazards and security vulnerabilities need to be considered (e.g. by the emphasis in different scenarios).

Contents

Figures

Tables

1 Introduction

One important aspect of Critical Infrastructures (CI) is their interactions and interdependencies. Unforeseen interdependencies might be a source of threat to systems and an important factor in our uncertainty of risk, particularly risk due to cascade failures in which the speed and size of loss is amplified. However interdependency is also central to providing tolerance to attack and failure—an important mechanism for adaptation and overall resilience.

Interdependencies can be addressed at a variety of phases, from planning and feasibility through to emergency or situational management. Interdependencies are sometimes considered according to the different perceived layers (e.g. of physical, control and supervisory management) and also in terms of abstraction such as effects, services and implementation. For each of these abstractions, there are a wide range of possible modelling approaches and theories that can be deployed, ranging from qualitative models, stochastic activity networks to complexity science style models and high-fidelity simulation. These can be deployed at a varying levels of detail, e.g. to model the detailed implementation topology or to model the service topology and cascading effects.

Interdependency analysis needs a sufficiently rich model for the analyst to discover and assess the risks. In particular, the following require consideration:

- Societal aspects need assessment as they provide possible hidden sources of commonality.
- Modes of operation have to be rich enough. Degraded modes of operation can amplify risks as levels of redundancy assumed at design time become defeated.
- Non-linearities in failure models (e.g. increased failure rates due to stress from nodes in the same locality) can lead to escalation and cascading effects.

Modelling and simulation results could be used to identify and evaluate vulnerabilities and consider the actions necessary for mitigating and preparing against these vulnerabilities in order to improve the overall resilience of the Critical National Infrastructure (CNI). Such analytical capability will be useful not only for the Government, but also for industrial stakeholders (e.g. utility companies).

CPNI, TSB and EPSRC have initiated this feasibility study in order to evaluate the current state of practice and research on interdependencies. In particular, the aim and objectives of Cetifs (CPNI, EPSRC, TSB Interdependency analysis Feasibility Study) is to assess the technical and commercial feasibility of

- the development of tools and services for analysing the interdependency between infrastructures, particularly information infrastructures, and assessing the associated risks
- establishing "Interdependency Analysis" as a distinct and recognisable service supported by tools and data

The study activities were grouped into two main phases:

- *Consultation and analysis phase*. Stakeholder consultations, a questionnaire survey, an extensive research review (in a separate report, see [28]) and incident analysis will be used to draw the "big picture"—the current state of practice and industrial maturity, and the state-of-the-art in terms of modelling, analysis and technology.

- *Synthesis phase*. Gap analysis will then evaluate the differences between tools and services, as well as the distance between current state of practice and state-of-the-art. In addition, gap analysis will determine the policy requirements, business models and research/innovation directions for the future.

Section 2 presents and discusses our findings from the analysis of CNI incident data. Sections 3 and 4 respectively present the initial requirements and current capabilities that have been identified during stakeholder consultations. Finally, Section 5 discusses the conclusions of this study and the resulting proposed strategy.

A preliminary research review has also been carried out, which is presented in a separate report [28]. That report presents an overview of network modelling, infrastructure simulation and visualisation.

2 Empirical evidence of infrastructure interdependencies

One could almost start and finish this section by pointing to the recent and continuing turmoil in the global financial sector to provide empirical evidence that the risks from interdependencies seem to have been ignored or misunderstood. It is not clear to what extent the risks were known and explicitly taken and to what extent they were underestimated. A survey of systemic risks in banking is provided by [8] and one might anticipate an avalanche of publications on the present situation.

While to a certain extent the importance of infrastructure dependencies is obvious (e.g. telecommunication need power, we all need money), we need to determine to what level dependencies and interdependencies are a significant contributor to the risks and to any lack of understanding.

Assessing the significance of interdependencies and the more general uncertainties in infrastructure interactions is a challenge, partly due to the complexity and scale of the systems that together make up the National Infrastructure (NI), and partly due to the lack of firm empirical evidence that can help us better understand cross-infrastructure vulnerabilities. The lack of evidence can be attributed to both the rarity of large, multi-infrastructure failures and the fact that smaller incidents tend to be poorly documented or not documented at all, leaving them as "anecdotal evidence".

In this section we provide an initial qualitative and quantitative analysis of incident data. Qualitative analysis of such failures can shed some light on dependencies and their complexity—on the other hand, quantitative analysis of several incidents can provide us with some indication as to how likely dependencies and interdependencies are to result in cascading failures across multiple infrastructures.

2.1 Qualitative analysis of incident data

2.1.1 Buncefield explosion

The explosion that took place at the oil storage depot located in Buncefield in December 2005 (the official investigation website, including subsequent reports can be found in [2]) has been characterised as the biggest explosion in peacetime Europe. While there were no casualties, the explosion affected the operation of multiple infrastructures (energy distribution, transportation, information infrastructure, finance, health as well as the environment) (see Figure 1).

This incident is of particular importance as it unveiled some important issues with regard to information infrastructures (II). We mainly focused our analysis on an IT

company/data centre named Northgate Information Solutions, which was severely affected by the explosion. The servers that were at these premises hosted patient records and admission/discharge for a number of hospitals in the area, a North London payroll scheme of approximately £1.4 billion, and systems/data for several local authorities [2], among others. We also took into account a report describing their business continuity activities immediately after the explosion [3].

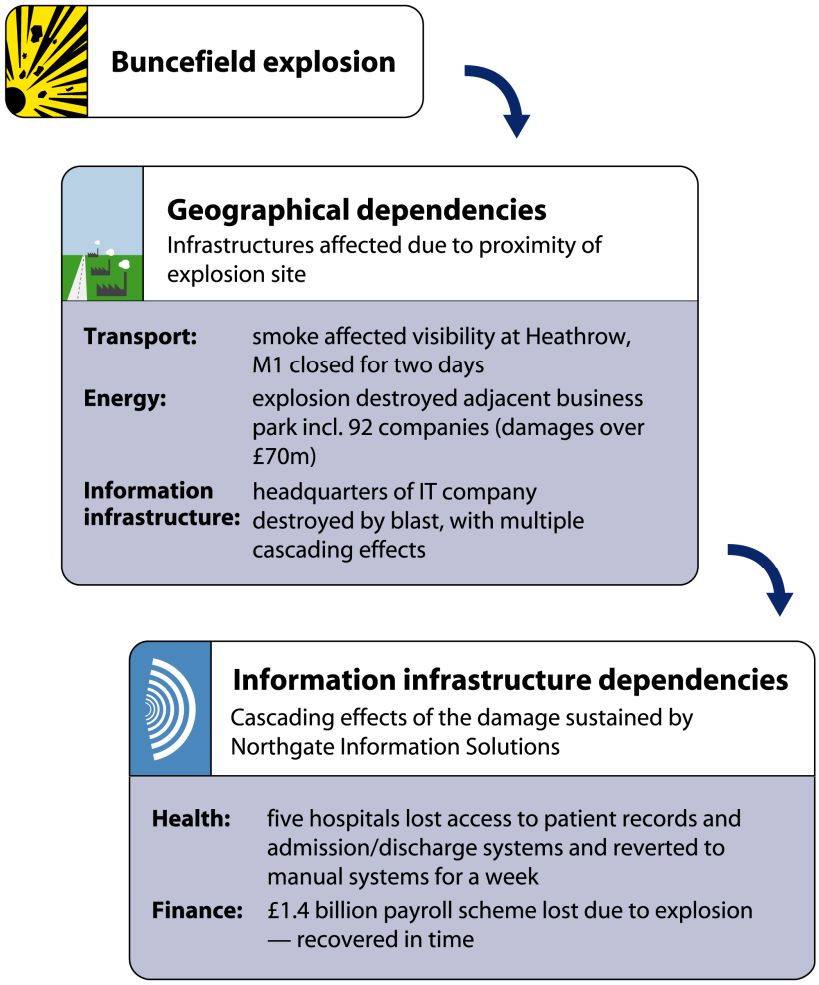

Figure 1: Buncefield explosion and cascading effects

Surprises and interdependencies

The explosion happened on a Sunday, at 6.01am. It is most likely that had this explosion taken place during working hours of a weekday, there would have been several casualties. The business park was empty at the time, but the 92 companies would probably be very busy with employees and visitors. Interdependency could then become visible between information infrastructure and health; had employees in Northgate Information Solutions been injured during the explosion, they would have been admitted to hospitals in the area, including Addenbrookes and the other four hospitals that were affected. The inability to provide healthcare services to people due to the loss of the information infrastructure would be a plausible and likely scenario. This interdependency becomes important as NIS employees were key in the restoration of the part of the information infrastructure that was lost.

2.1.2 2007 UK floods

The floods that struck much of the country during June and July 2007 were extreme, affecting hundreds of thousands of people in England and Wales. It was the most serious inland flood since 1947 [1]. 13 people lost their lives, approximately 48,000 households and nearly 7,300 businesses were flooded and billions of pounds of damage were claimed. In Yorkshire and Humberside, the Fire and Rescue Service launched the "biggest rescue effort in peacetime Britain".

The floods affected multiple infrastructures, such as water and food supply, power, telecommunications and transportation, as well as agriculture and tourism. Many businesses also suffered flooded sales premises, together with damage to stock and equipment. Figure 2 depicts some of the cascading effects that resulted from the floods.

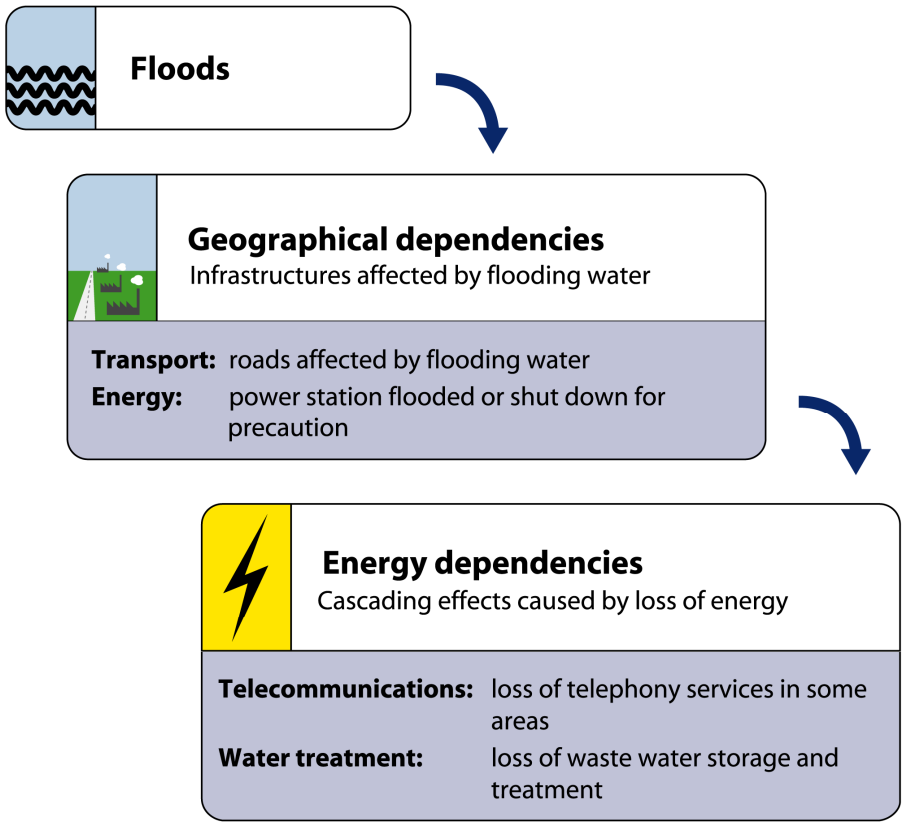

Figure 2: Cascading effects during the 2007 UK floods

The levels of rainfall in summer 2007 were generally well predicted by the Met Office—in particular, the weather forecasts preceding the major July flooding were the most detailed and accurate to date for a major flooding event in the UK. Subsequent focused warnings about the areas at greatest risk of disruption were provided as confidence in the forecasts grew.

Although the Met Office provided early warning signs, and it is acknowledged that the Environment Agency has advanced capability for mapping and analysing the risk of flooding in the UK, the dependencies and interdependencies across infrastructures were not well understood beforehand.

Surprises and interdependencies

In addition to the cascading effects shown in Figure 2, there were also some examples of unexpected dependencies. One was the potential failure of the Ulley Reservoir [18]; once fears that the dam was going to collapse started to emerge, it was decided to turn off many of the essential services in the inundation zone as a precaution. Although concerns about cracks on the dam had been reported in the past, they had neither been addressed by reinforcing the dam, nor by analysing and preparing to deal with the consequences of losing the dam.

Interdependency concerns emerged in some incidents that occurred during the floods as well. One example was in Hull [15], where the pumps protecting the city flooded and failed but there were some localised instances where loss of electricity through flooding caused the loss of pumps and therefore further flooding.

2.2 Quantitative analysis of TNO data

The Dutch TNO has provided us with data regarding 203 infrastructure incidents in the UK. They cover approximately 6 years of data based on media reports. Of the 125 incidents recorded by TNO, 19 propagated to another infrastructure.

We have developed a stochastic model of cascade failure and fitted the data using a maximum likelihood technique to develop a prediction of the probability of larger cascade failures. The results are shown in Figure 3 below. The two lines represent different modelling assumptions. In one model, an unobservable quantity "size" variable was assumed to exist for each tree affecting the likelihood of cascade events (edges) occurring within it (i.e. making it likely to be a larger or a smaller tree). The other model assumes that there is no variation in size.

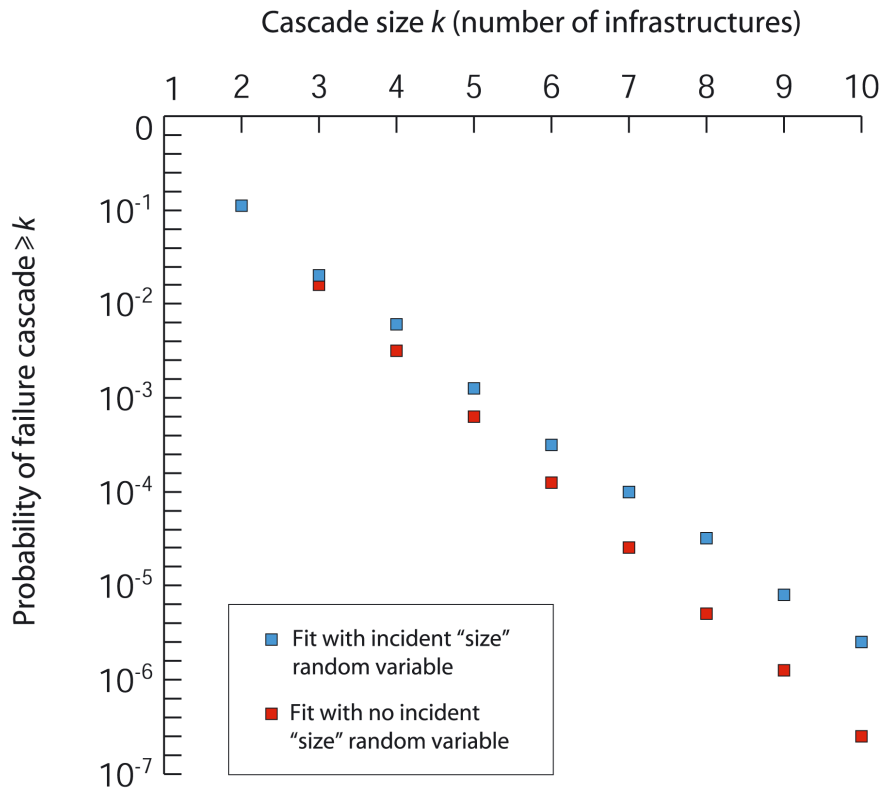

Figure 3: Prediction of probability of cascade infrastructure failure

The model predicts that there is a near exponential relationship between event frequency and the number of infrastructures affected. Note that cascade within one infrastructure is counted as size 1, but propagation of failure from one infrastructure to another, and then back to the original (which is an interdependency), the cascade size is 3.

The disruption and complexity of recovery is very dependent on the number of infrastructures that are impacted (contrast for example the response in California to forest fires to the impact of hurricane Katrina).

We have not conducted any modelling or analysis yet of how we might model the costs of these infrastructure cascades and assess the seriousness and potential savings. We would need some approximate data on

- How the costs varied with *k* (probably faster than linear). We might draw an analogy with Metcalfs Law that the value of a network is proportional to the square of its size.
- How the time to recover varied with the number of infrastructures impacted (again this might be very non-linear due to the complexities of recovering from multiple infrastructure failures) and how the costs vary with duration of incident.

Modelling infrastructure interaction is essential if we are to understand and mitigate these costs. However as there are so many potential scenarios of combination of events this will probably require both more work on defining plausible scenarios and also some real-time capability to model and assess specific incidents. The level of detail and type of modelling capability that might be required is discussed in Section 4. Some of the CNI analysis and protection capabilities we have seen have an interface to macro-economic impact and there are a number of studies in the literature on the economic impacts of infrastructure failures [24].

This modelling is of course approximate and can only be as good as the dataset on which it is based. It is one of the observations from this study that the responsibility for data collection is unclear; it seems that some systematic attempt should be made to collect consistent data so that the importance of incidents can be assessed and lessons can be learned.

2.3 Anecdotal evidence

During discussions with expert stakeholders (and especially with utility companies and infrastructure operators) it became clear that many had experience of interdependency "surprises", despite them being well informed and aware of the issues. In addition to those, we also came across incidents in the press or in research publications. We have therefore taken these incidents into account, although we do not have sufficient information for an analysis to the same extent as Buncefield, the UK floods and the TNO incident data set.

One example was an incident concerning a fire in deep level tunnels running beneath the centre of Manchester, which caused severe damage to telephony cables, causing major disruptions to telecommunications in the region. It was estimated that approximately 130,000 homes and businesses in the city were affected. Emergency services were among these; reportedly, the Manchester Ambulance Service was hit, while the 999 service could not be dialled by people in an emergency. In addition, several banks and airlines were said to have lost access to their systems, while Vodafone had lost some of its

network. Other utility companies were affected, such as Powergen, whose website was down for days [6].

2.4 Discussion

Incidents such as the Buncefield explosion and the 2007 floods are rare, and it can be argued that it is unlikely similar occurrences will take place in the near future. Nonetheless, their analysis can help us understand several aspects of infrastructure dependencies and interdependencies which may emerge in the future, even if in different context and scale. This section highlights some the themes that have come up during these incidents; aspects that were deemed as surprises even though they would seem to be known in principle and, to a certain level, understood by infrastructure owners and Government.

Geographical dependencies. Figure 1 and Figure 2 outline some of the geographical dependencies that emerged in Buncefield and the floods respectively. Geographical dependencies are, to a certain extent, known, as the identification of physical proximity of assets is straightforward, especially when we consider an area surrounding a plant or within a flood-vulnerable area. Nonetheless, there were still several surprises in these events (for instance, during the floods, several critical services had to be shut down for precaution in case the flood reached them but there was uncertainty as to whether that was actually needed or not). Such dependencies concern not only risks associated with direct impact from a blast, but also more complex and indirect consequences. The effect the Buncefield explosion had on the adjacent business park and the data centre in particular was also deemed as a surprise. These dimensions of the two major incidents illustrate that analysis is required in order to better understand geographical dependencies and how they can result in cascading failures.

Competition for resources. This challenge arises during an incident and can also lead to interdependencies or further cascade effects. Although capacity and bandwidth of resources may be known to infrastructure owners, during crises they may be reached very quickly, and in unusual ways. Competition for resources can also manifest when an asset that provides a resource is lost (e.g. a power station), where other dependent nodes will have to find alternative suppliers.

Long term effects. In some cases, major incidents can involve significant long term loses to infrastructure and economy by complex cascade paths. One typical aspect of this is the effect a disaster can have on tourism. In the Pitt review there was an extended discussion on the role of media following the floods and the long-term effect on tourism and the economy of affected areas. Although there are a number of studies in macro-economic impact of infrastructure failures, the long term effects of such disasters and how they can be controlled are aspects that are not well understood and require more detailed analysis, considering various parameters such as the role of media.

Cascading effects and recovery. The analysis of the TNO data resulted in some important conclusions with regards to cascade failures and the impact they have on recovery. However, we have not been able to extend the analysis to assess potential costs.

The issues discussed in this section are a selection of challenges that emerged in incidents and are intended to serve both as an introduction to the importance of interdependencies but also to inform our later assessment of required capabilities. The

lack of incident data and systematic qualitative and quantitative analyses hampers our understanding of the issue. This is due to the comparative rarity of events, and the difficulty in attaining data from multiple organisations, with many incidents going unreported or kept as anecdotes within one infrastructure.

3 Critical Infrastructure and interdependencies—initial requirements

In the first phase of the project we consulted with a range of stakeholders from government and industry (mainly utilities) in order to assess their understanding of the challenges of infrastructure interdependency, their current approach to CNI protection, the context of their operation in terms of policy and regulation, and their further requirements for analysis and modelling. This section summarises and discusses the perspectives of these stakeholders.

3.1 Critical infrastructures

In the UK, the Critical National Infrastructure (CNI) is defined as

> ".. those key elements of the national infrastructure which are crucial to the continued delivery of essential services to the UK. Without these key elements the essential services could not be delivered and the UK could suffer serious consequences, including severe economic damage, grave social disruption, or even large scale loss of life".

The EU has a very similar definition:

> "A critical infrastructure (CI) consists of those physical and information technology facilities, networks, services and assets which, if disrupted or destroyed, have a serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of governments [25]".

While there is some debate over what is considered a "critical sector", the following are covered within the European Programme for Critical Infrastructure Protection (EPCIP):

- Energy
- Nuclear industry Information, Communication Technologies, ICT
- Water
- Food
- Health
- Financial
- Transport
- Chemical industry
- Space
- Research facilities

There are also proposals to include "building structures" and "areas of mass congregation" and some agencies even consider sporting events such as Euro2008 within CIP.

3.2 Interdependency service oriented perspectives

A key notion is that an infrastructure provides a *service*. The functioning of one CI's service often depends on the functioning of another (dependency), e.g. mobile phone transmitter requires electric power and sometimes they can be mutually dependent (interdependency). For example, water needs electricity for pumping, and a power station needs water to start-up. The services can be coupled by

- function—as in the example above
- resources—common resources such as fuel, water, people that are consumed or used by each service
- shared or common sub-services

In addition, other factors can cause failures to be coupled—so that if we see the failure of one service we are more likely to see the failure of the other. This can be due to

- common environmental factors (geographical co-location causing environment coupling)
- common components that might fail at similar times (types, specific) or have common vulnerabilities that attract coincident attacks
- similar assets that also attract coincident attacks (e.g. computer viruses)

There can also be further mechanisms propagation of failure from one service to another via

- pollution of resources (e.g. poisoned messages propagating in a computer network)
- stress or damage propagation (e.g. physical blast, local overload causing stress in neighbours and inducing failures)

The propagation of failure can lead to cascades with rapid escalation of damage. In addition, the services are implemented across a range of contractual, organisational, commercial, legal and political boundaries giving rise to a complex set of ownerships and responsibilities. This provides further possible coupling and dependencies due to e.g. organisational or maintenance deficiencies, or operational constraints of failure recovery or isolation.

3.3 Resilience perspective

Interdependencies are often discussed as a source of threat to systems. Indeed this can be the case and in particular unforeseen interdependencies can be a source of surprise and uncertainty in our ability to understand risks and system behaviour. However interdependency is also central to providing tolerance to attack and failure, a means for adaptation and overall resilience. *Resilience* provides a useful framework within which to consider different stakeholder approaches, requirements and responsibilities for critical infrastructure services.

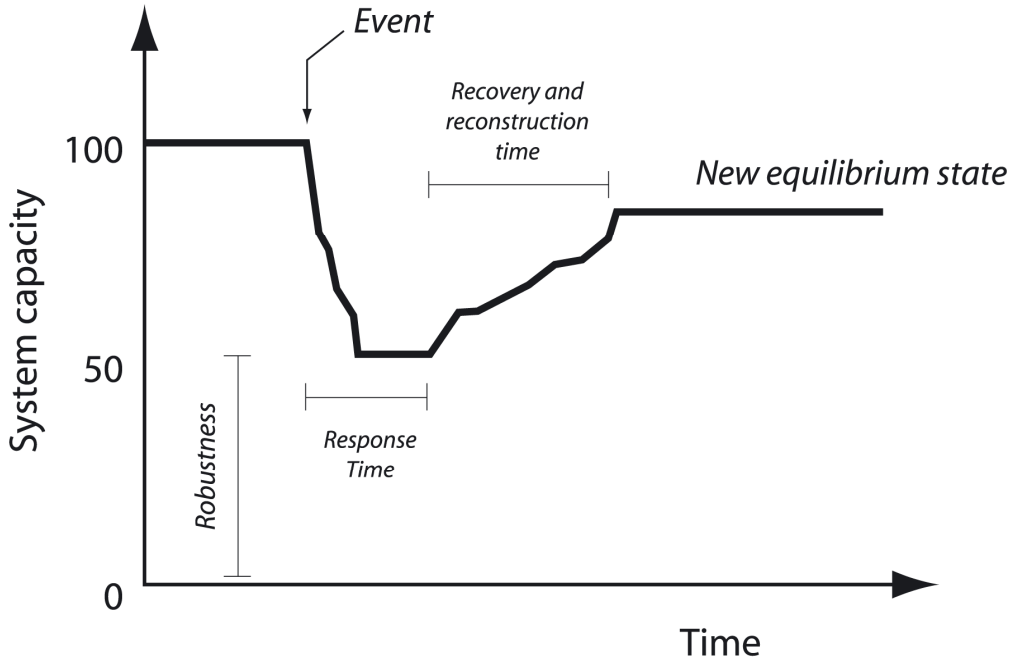

Figure 4: Resilience

Resilience has its common sense meaning but is used in a variety of ways. The US Department for Homeland Security (DHS) and UK Resilience viewpoints consider the loss due to an incident as an indication of how resilient a system is—this is shown in Figure 4. However in [17] the emphasis is on the ability of a system to adapt and respond to changes in the environment. In a recent report for the Defence Science and Technology Laboratory (DSTL) [16] produced by CSR, City University London, two types of resilience were distinguished:

- *Type 1: Resilience to design basis threats*. This could be expressed in the usual terms of availability, robustness, etc.
- *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.

Some policies consider an "all hazards" approach that addresses both malicious and accidental attacks on systems (e.g. in EU CIP Directives [29]). In addition, the notion of *dependability*, or dependability and security, as an umbrella term is useful to capture the need to address all attributes (safety, security, availability etc.) rather than just a single attribute.

So the overall service level view is summarised in Table 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

The different stakeholders all had an interest in resilience but had very different emphases. Broadly speaking these concerned the scope of their responsibilities, whether it was:

- *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 CNI.

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

We can use the resilience-dependability framework to capture the different perspectives of stakeholders. For example, those of CPNI and Civil Contingency Secretariat (CCS) are shown in the table below.

Framework component	Stakeholder: CPNI	Stakeholder: CCS
What services are addressed?	All within scope of NI suitably prioritised	All
Which dependability attributes are concerned?	Classic security attributes – confidentiality, integrity, availability	Emphasis on availability
What range of hazards/threats?	Security related only	Natural hazards in terms of initiation. Advice from CPNI on security All hazards in decision and recovery phases
Which resilience phase?	Emphasis on prevention and preparation and learning phase. Advice to CCS during incidents	National risk assessment deals with long term losses Emphasis on recovery and incident management

Table 2: CPNI and CCS perspectives

A security evaluation could then be seen as evaluation of resilience for certain threats (e.g. malicious ones) and for certain attributes (confidentiality, integrity, availability). The evaluation of the security part of resilience would then address the different stages of Table 1.

In this study we are particularly interested in (inter-)dependencies, and so we can use the framework to assess what dependability attributes, what resilience phase and what threat scope is of concern and being addressed by particular modelling and analysis approaches.

3.4 Information Infrastructures and interdependencies

The focus of much of the debate and research on critical infrastructure is around the more classical power infrastructures. However information infrastructures can be an important source of interdependencies and surprises. The term "Information Infrastructure" was originally coined in 1993 in the US. More recently the Organisation for Economic Co-Operation and Development (OECD) has offered the following definition. According to [OECD/EU],

> *A critical information infrastructure (CII) consists of those information and communication technology facilities, networks, services and assets which, if disrupted or destroyed, either (1) have a serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of governments, or (2) causes the functioning of a critical infrastructure which it supports to be seriously disrupted.*

The definition recognises the importance of information infrastructures in their own right but also their role at the heart of the other infrastructures. Within the EU the European Commission's Study on the Availability and Robustness of Electronic Communications Infrastructures (ARECI) report [9] provides a review on the availability and reliability of the European Information Infrastructure and identifies eight components:

Environment: Communications systems are in the physical universe and as such, operate in various environments. These environments range from temperature controlled buildings to installations exposed to harsh conditions such as outside terminals and cell towers that are exposed to inclement weather, trenches where cables are buried, space where satellites orbit, and the ocean where submarine cables reside.
Power: Without electrical power, electronic systems are lifeless. The power required for communication networks includes the internal power infrastructure, batteries, grounding, cabling, fuses, back-up emergency generators and fuel, and commercial power.
Hardware: The electronic and physical components that comprise the network nodes, including the hardware frames, electronics circuit packs and cards, metallic and fiber optic transmission cables, and semiconductor chips.
Software: Today's complex communication networks gain their power and flexibility from the computer code that controls the equipment. This category covers all aspects of creating, maintaining, and protecting that code, including physical storage, development and testing of code, version control, and control of code delivery.
Networks: Networks include the various topological configurations of nodes, synchronisation, redundancy, and physical and logical diversity.
Payload: The purpose of a communications network is to deliver some form of communications, be it voice, data, or multimedia. The payload category includes the information transported across the infrastructure, traffic patterns and statistics, information interception, and information corruption.
Human: Humans operate the network and present one of the most complex dimensions to analyse. The human ingredient includes intentional and unintentional behaviours, physical and mental limitations, education and training, human-machine interfaces, and personal ethics.
Policy (or ASPR): Policies include any agreed or anticipated behaviour between entities, such as companies or governments. They include Agreements, Standards, Policies and Regulations (ASPR) and provide a framework that defines the expected interaction between government and the communications industry.

Table 3: Components of Information Infrastructure from the ARECI report [9]

Within the information infrastructure there are many sub-sectors such as:

- Information systems and network protection
- Instrumentation and control systems (SCADA)
- Fixed communications
- Mobile communications
- Radio communication and navigation
- Satellite communications
- Broadcasting

There are complex intradependencies[1] between these sub-sectors. Some of these are illustrated in Figure 5 below.

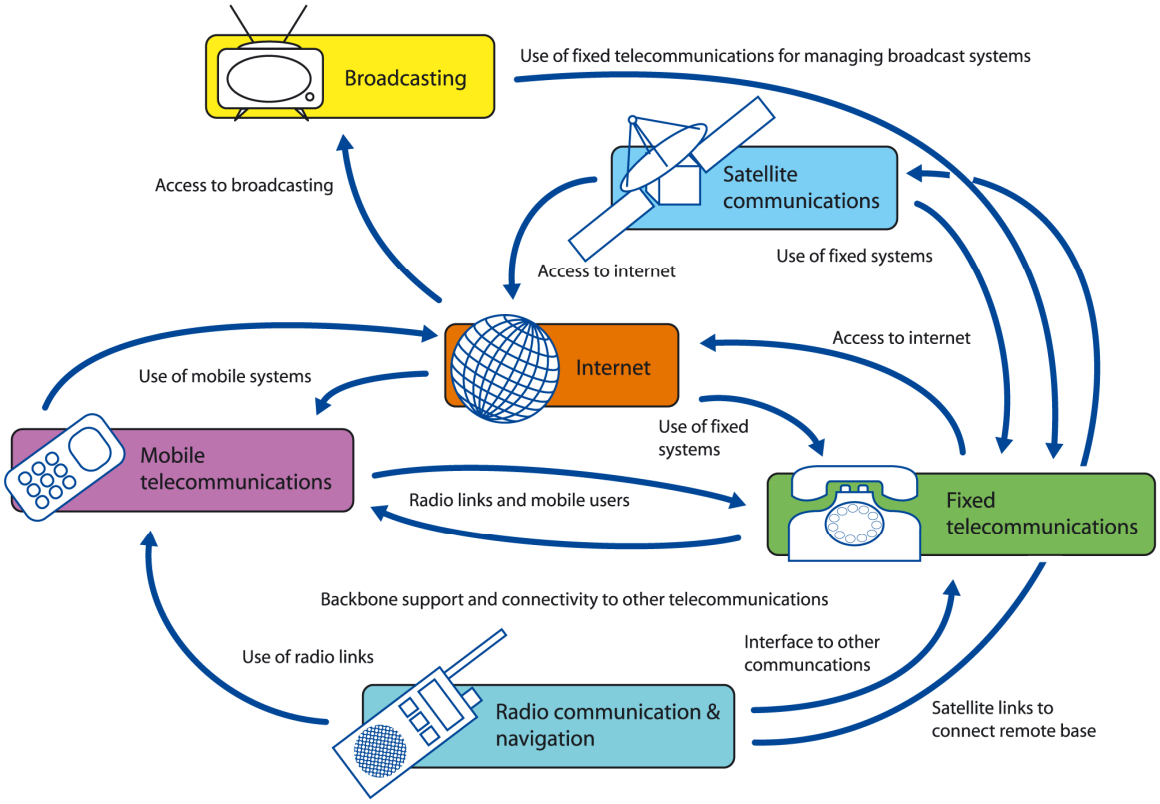

Figure 5: Example of Information Infrastructure intradependencies (from [11])

Overall, it can be argued that information infrastructures could be seen in two dimensions. On the one hand, we need a *service oriented view* and this is not simple to extract from the architecture of the different communication and information technologies. On the other we need to understand *information and data* (not just communication networks) and associated meta-data, such as criticality, form (i.e. electronic or paper-based), and location.

Information infrastructures provide significant challenges. Some challenges are the same as with other infrastructures but exacerbated by complexity of systems. Others are due to

- speed of structural change and innovation so that historical resilience replaced and organisational and contractual complexities introduced
- intertwining of services within the Sector (mobile operators dependent on fixed services, ISPs dependent on communications)
- co-location of different infrastructures at a physical level e.g. shared ducts, server farms close to power
- difficulty to tell if a service is corrupted or if it has been attacked or exploited

Another challenge that is posed by Information Infrastructures (II) comes from the nature of the technology itself. This means there can be a dynamic, uncertain allocation of service to IT infrastructure. While for example, there may be some choices of the way

[1] In this report we do not distinguish between intra- and inter- dependencies

water reaches a house from different reservoirs and sources, there is rather limited flexibility. In the II a service—such as a point to point communication—can be routed dynamically across a variety of organisational, legal and national boundaries. Of course, the operators of the more critical assets are well aware of these issues and they strive to ensure that the redundancy and diversity of communication services are not compromised by some unforeseen dependency; nonetheless, in the consultations it became clear even the most mature infrastructure operators have difficulties in establishing this. For other less critical systems, it is doubtful that they have the resources or business strength to do this. Even well organised utilities can have surprises—for example, that two suppliers had acquiring bought connectivity from the same third supplier during maintenance and introduced a single point of failure into the system. In addition we have anecdotal evidence of connectivity surprises within a major international energy company where prior to an evaluation only 10% of computers were thought to be connected to the Internet, but after evaluation this figure rose to 90%

There is a need to identify these situations and to understand the risks involved and to look at design measures and applications that can make service dependability explicit e.g. by making explicit routes and provenance of services.

3.5 Non-technical, intangible, infrastructures

One other aspect that came up in our consultations is the importance of "soft" intangible critical infrastructures, e.g. trust and confidence within society both in their own right and as an important component that is essential to the functioning of critical services. For instance, trust between individuals, between individuals and organisations and between these and the representative of the state is essential for the delivery of service. This, as with so many of the infrastructures, is often hidden but comes to the fore in times of crisis and recovery from disaster.

Trust is an asset that can be built-up, destroyed, squandered and undermined as with so many other assets and resources. If we are to assess interdependencies we need to take into account these essential yet softer aspects and their relationship to the more tangible aspects. This assessment should be cognisant that these soft aspects are just as much the target of security threats as the more obvious physical and cyber systems. Indeed it may be that a patient and well read adversary would have a strategy that would be aiming at these assets. For example, the financial infrastructure relies very heavily on trust in the banking system for it to function at all. Witness the latest credit crunch, the Northern Rock bank crisis and also public trust in government announcements and the panic buying of petrol because people did not believe assurances about supply. An adversary strategy that relies on people legitimately taking their money out of a bank is far more effective than any physical raid on the bank (unless one wants to get rich). At a micro-level, social engineering attacks that exploit people's willingness to give passwords away can be seen as a form of attack exploiting confidence.

While in the past the soft infrastructure might have been separable from the more technical infrastructures they are clearly related. Trust in the competence of government and authorities is dependent on how well they cope with crises and incidents in both the physical and soft infrastructures. Moreover trust relationships that citizens have between themselves, organisations, government and agencies are strongly dependent on the information infrastructure: a trend that is likely to increase (see the transformational government agenda [7]).

Assets such as trust and privacy within society are important and can be seen as emergent properties; although they are affected by local aspects of trust they have a

complex relationship to localised issues. Trust in organisations and government may exhibit the classic complex systems phenomenon of rapid transitions and "tipping points".

3.6 Industry practice and viewpoints

In addition to the in-depth consultation, we conducted a questionnaire-based survey in order to improve our understanding of the current level of maturity and awareness of dependency issues in the industry. From the responses we have received, we found that utility companies address the challenges of infrastructure interdependencies by ensuring close relationships with suppliers and vendors. They believe that close relationships can assist in understanding the various risks associated with their providers' failure and their overall level of resilience. Risks are monitored through internal risk review groups, and company boards oversee the results. Also in some cases utilities hold industry forums to exchange information, or engage in regular review meetings. Exercises involving suppliers have also been carried out. In some cases, alternative providers have already been sourced as part of contingency planning.

However, the protective measures to be taken depend on the nature of the risk or vulnerability and on the particular department. Overall, utility companies focus on improving resilience by having business continuity planning, frequent risk assessment, back up systems (especially for IT), as well as security technologies.

One interesting finding is that there is no single point of contact for the assessment and mitigation of vulnerabilities related to infrastructure interdependencies. Responsibilities are distributed across the corresponding departments that deal with each infrastructure. IT services obviously bear much of the responsibility for ensuring continuity of the computer-based information infrastructure. This may also involve crisis management or risk management departments.

Although infrastructure dependencies are considered in risk assessment, this is mostly done in more traditional ways, without tool support. In one case, it was suggested that mapping software was used, although just once, for examining proximity of functions to cable routes. In addition, none of the respondents were aware of any technical documentation, research or conferences in infrastructure interdependency, something which perhaps suggests the presence of a gap between research and practice.

Most responders suggested they had experienced either minor or major disruptions due to failure of other infrastructure providers.

The questionnaire also probed whether there was scope for some form of Interdependency analysis as a distinct service. There was no consensus from respondents; some believed it could be, and some suggested they would be interested if it was part of a wider, risk assessment service. The issues of trust and confidentiality were raised as serious obstacles.

3.7 Preliminary stakeholder requirements

In terms of capabilities, the main conclusions from discussion with stakeholders are the following:

1. There is recognition that interdependencies are part of wider issues of understanding infrastructure interaction.
2. They are concerned that they lack knowledge of infrastructure interactions.

3. There is sufficient expert judgement, anecdotes and incident analysis to suggest that this lack of knowledge may present a significant risk or a missed opportunity for improving resilience at all stage of the resilience lifecycle.
4. They see many potential advantages in a more sophisticated approach to infrastructure modelling but at present they do not know under what circumstance these uncertainties are significant and so can not justify the required investments.

In discussion with stakeholders we have identified requirements across various areas that relate to infrastructure interdependencies. These areas are the following:

- **Inherent infrastructure resilience—scope and overall methodology:** Perspectives here address the level of resilience that is built in to infrastructures and normal operation.
- **Infrastructure analysis and support:** The consultation identified a number of different possible service delivery perspectives.
- **Hazard and vulnerability identification and management:** Perspectives vary on the scope of hazards to be addressed or the approach to the management of systems.
- **Resilience phases:** Potential capabilities and requirements that concern the various phases of resilience.
- **Critical information infrastructures:** A greater focus is given in this study to CII.
- **Dependability of the modelling:** An integral part the development of tools and analytical services is to ensure that they are dependable. There will be a need to trust the results of infrastructure modelling and analysis and possibly integrate information from a variety of trusted and less trusted sources. There will therefore be a variety of confidentiality requirements on the modelling tools and supporting IT infrastructure depending on their application and mode of service delivery. Unless these confidentiality requirements are met the modelling activity could provide a threat.
- **Evidence of costs and potential benefits**: Cost and benefit issues have to do with costs of failure and benefits of interdependency analysis.

A summary of the preliminary requirements is provided in Figure 6, below.

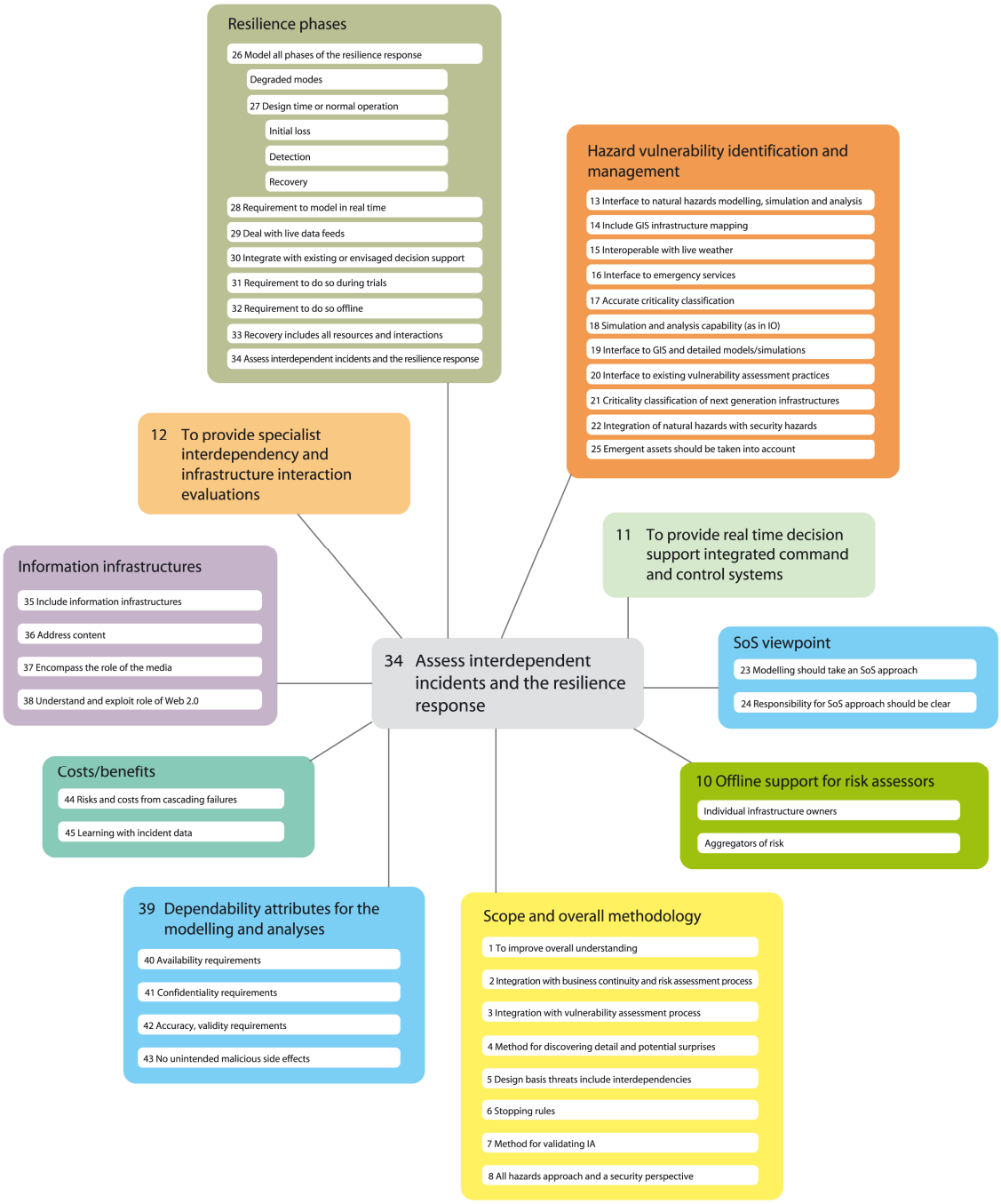

Figure 6: Overview of preliminary requirements

In the next section we review the current state of infrastructure modelling so that we can recommend possible strategies for addressing these preliminary requirements and developing a clear view of the way ahead.

4 Modelling, simulation and analysis—capabilities

Providers of infrastructure modelling and/or (inter-)dependency analysis are either government-endorsed organisations, or leading private technology solutions providers. Overall, they offer a diverse range of services. Our consultations have aimed at understanding their capabilities and market deployment approaches. These will then be related with, and contrasted to, the initial requirements in the next section.

4.1 Introduction

The overall architecture of infrastructure modelling is illustrated in Figure 7. There are a range of modelling, simulation and analysis techniques or models that provide the insights into the interdependency or infrastructure interactions. These require significant, and perhaps confidential, information and data on the topologies and properties of the systems and their control strategies. The application of the models needs to be embedded in a methodology and there needs to be the right level of interaction with users and other stakeholders, hence the visualisation component.

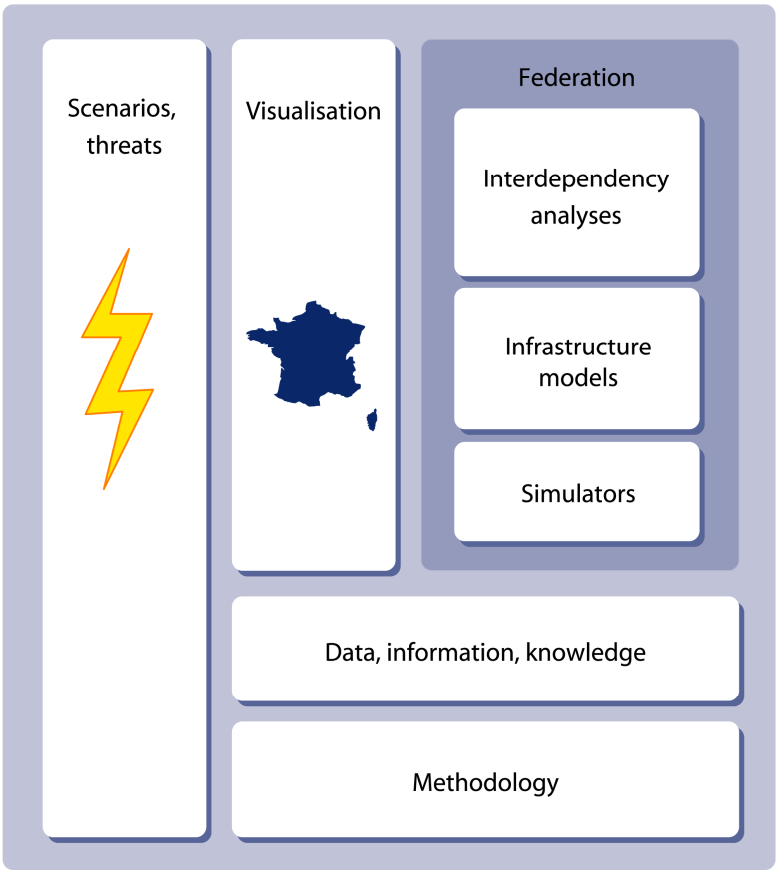

Figure 7: Modelling components

The components of Figure 7 are explained as follows:

Infrastructure models. Modelling within a single infrastructure or system is a diverse and mature field. Models are fundamental to understanding system behaviour, evaluating risks and designing operational strategies. The electricity, nuclear, telecoms networks sectors all have significant modelling capability as do those concerned with environmental causes and impact. The issues for this study revolve around how we can

exploit this expertise effectively and efficiently to gain an understanding of infrastructure interactions and risks.

Simulators. Simulation is the imitation of some real thing, state of affairs, or process. The act of simulating something generally entails representing certain key characteristics or behaviours of a selected physical or abstract system [26]. The US DoD Modelling and Simulation Coordination Office defines simulation simply as 'a method for implementing a model over time' [27]. Simulation may either be only an execution of a model over a period of time, or it may be interactive, with the human in the loop.

There are many different types of computer simulation—the common feature they all share is the attempt to generate a sample of representative scenarios for a model in which a complete enumeration of all possible states would be prohibitive or impossible.

Simulation is often referred to in the context of live, virtual and constructive:

- Live simulation (where real people use simulated (or "dummy") equipment in the real world);
- Virtual simulation (where real people use simulated equipment in a simulated world, or virtual environment), and
- Constructive simulation (where simulated people use simulated equipment in a simulated environment).

The provision of live and/or virtual capabilities within infrastructure simulation depends upon the stakeholder requirement for real-time analysis, decision support and disaster management.

Interdependency modelling can be considered according to the different perceived layers (e.g. of physical, control and supervisory management) and also in terms of a range of abstractions from high-level services to detailed implementations. For each of these abstractions, there are a wide range of possible modelling approaches and theories that can be deployed, ranging from qualitative models, stochastic activity networks to complexity science style models and high-fidelity simulations. These can be deployed at a varying levels of detail, e.g. to model the detailed implementation topology or to model the service topology and cascading effects.

Federation refers to the integration of several simulations (federates). This is primarily done through achieving interoperability among separately developed simulators. Standardisation is required in order to define common elements.

Data, information and knowledge. This refers to the data that is fed into the simulation. Data can be either static or live. For instance, simulators are often linked to live weather feeds, GPS and other forms of live data sources. Data acquisition and verification are important challenges as insufficient, incorrect or inaccurate data can result in a misleading analysis. Information and knowledge can take the form of intelligence, i.e. meaningful data that is needed to guide or focus an analysis.

Visualisation refers to the graphical representation of the modelling and analysis. This can be either on a standalone PC screen, or on large, operating room screens, or over a set of various screen types, sometimes even distributed across various locations. Geographical Information Systems (GIS) are a typical example of visualisation. In interdependency analysis, visualisation tends to be layered, with several filtering options to guide decision support and communication.

Methodology. A defined and structured approach can assist in an efficient and effective modelling and analysis. The methodology contains aspects of requirement elicitation, data gathering and analysis, modelling, simulation and the eventual development of conclusions and decision support.

Scenarios and threats. Scenario development considers situations and sequences of events that are of particular concern, in order to identify threats and gain insight of the 'system' behaviour under hazardous conditions. In most cases, a 'reasonably' worst case scenario is needed in order to focus planning and mitigation against a threat that has a realistic likelihood of occurring.

4.2 Current capabilities

We consulted various private companies or foreign and UK Government agencies that offer tools and/or services that fall under one or more of the components of the infrastructure interdependencies architecture that was presented in the previous section. Consultations aimed at understanding what the state-of-the-art is in terms of modelling and analysis and what business models they deploy to commercially exploit their capabilities.

In particular we consulted with

- *Government agencies:* The Government agencies we consulted are made up by multi-disciplinary teams (engineers, IT experts, sociologists, psychologists etc). They have advanced infrastructure modelling but primarily do off-line decision support. They work closely with industry (mainly utility companies) for acquiring data. In some cases, Government agencies offer services to industry to support their contingency planning in case of large disasters (such as the Australian 'Critical Infrastructure Protection, Modelling and Analysis' (CIPMA)).
- *Private companies:*
    - *Integrated services*: Companies with an advanced technological infrastructure and appropriate expertise and experience that move into the area of interdependency analysis from relative fields (e.g. safety, risk assessment). Such companies may support Government for vulnerability identification and assessment as well as training.
    - *Simulation*: Simulation experts have the expertise to develop models and tools for simulating infrastructures and creating federated simulations in order to explore interactions and interdependencies. There is considerable experience and expertise in general simulation capabilities for domain or platform specific systems and each infrastructure has simulations specific to its own domain (but not generally integrated with other infrastructures). Simulation is a broad and mature field that can readily contribute as a component of interdependency analysis.
    - *Asset management:* Asset management is the process of identifying and recording assets along with the necessary information about them and can be employed to discover dependencies and interdependencies among critical assets. However, this practice is rather information-intensive and time consuming. The approaches used in asset management may be used to address some of the perceived problems with Information Infrastructure of not knowing the relationship between services and physical assets. There

was some scepticism from the IT infrastructure owners that asset management could solve these issues.

- *Geographical Information Systems*: GIS is a growing area of research and practice, focusing on the storing, management, analysis and visualisation of geographic information. With the appropriate level of detail, GIS can be used to identify geographical dependencies. For instance, with information regarding topologies of electricity and gas networks, the analyst can identify areas where cables are too close to gas pipelines. Overall, GIS applications can support both off-line and real-time analysis and decision making. GIS tools can address many of the aspects of the model architecture but currently interdependency modelling is limited.

4.3 Research overview

The models and simulations developed to support infrastructure modelling and simulation are diverse and complementary. There are multiple ways in which these models are related and there is no single taxonomy or classification that suits all purposes.

As part of this study we have undertaken a review of related research. This is reported in more detail in a companion report [28]. In the review we focus on the results of the models to provide a basis for describing relationships between them. The classification of modelling activities from this perspective, applied in particular to models, tools and methodologies is provided in [28]. This includes:

- *Abstraction level and model boundaries:* Questions such as "how much of the real world should be modelled?" constrain modelling methodology and the applicability of modelling results. A continuum of possibilities exists ranging from high-fidelity (very detailed) simulations to mid-range and low-fidelity models;
- *Technique and underlying theory:* (Inter)dependency analysis of complex systems has been recognised as an inherently interdisciplinary activity. There exists a wealth of experience and knowledge relevant for (inter)dependency modelling. This column in the table below gives information about established formalisms, theory and techniques used in building and analysing the models;
- *Model applicability:* The type of problems where the model can provide useful support is indicated in this column and the extent of tool support.

The following table provides an overview for the research landscape as detailed in a separate report [28]. (The order in the table does not reflect priority or maturity).

	Abstraction level	**Theory**	**Applicable results and tools**
Qualitative and semi-qualitative models	*Model entities:* Varying from Mid to High level Nodes and links; Nodes (Systems or system components) and links (correlations, logical, functional or physical dependence) *State Space:* Continuous	Continuous time Stochastic processes, Stochastic Activity Networks	Rapid dependency identification and analysis; Model scoping; Provides estimates for stochastic measures related to CI operation, including the likelihood of occurrence, extent, and duration of events in CI. MODAF tools, ASCE, Möbius,

	Abstraction level	Theory	Applicable results and tools
	or discrete, diverse		and bespoke research software.
Leontief-based model	*Model entities:* Nodes (Systems or system components) and links (logical, functional or physical dependence) *State Space:* Continuous, homogeneous	Graph theory, causal networks	Study of failure spreading behaviour; formulation and study of recovery strategies. Models of macro-economic loss. Bespoke tools
Indicative system dynamics models	*Model entities:* Nodes (Systems or system components) and links showing influence *State Space:* Continuous, homogeneous	System dynamics	Exploratory behaviour often at a high level of system behaviour based on dynamic models of how nodes interact. Often representing high-level services Tools such as Gamma
Topological and network models	*Model entities:* Nodes (Systems or system components) and links (logical, functional or physical dependence) often generalised as influence. Limited infrastructure functionality but detailed topology.	Graph theory, causal networks Network topology and theories Systems dynamics Computer science – FSA	Many examples of graph based models showing interaction of nodes. Work on resilience of electricity networks using topological measures of risk and comparing these with functional measures. A variety of tools and algorithms for finding topological properties of interest.
Stochastic analysis of interacting networks	*Service level, Nodes:* (at power side: primary and secondary substations; at telco side: ADM, Local Exchanges, Transit Exchanges) *Links*: (at power side: electrical trunks; at telco side: optical rings, copper), Failure and repair rates Also for Common-mode failure model can have higher level of abstraction *Model entities:* Mid level *State Space:* Continuous or discrete, diverse	Binary Decision Diagrams, Stochastic Activity Networks Flow models, congestion modelling, Continuous time stochastic processes	Estimating stochastic indicators of the quality of service provided by interconnected, interdependent networks, including the likelihood of occurrence, extent, and duration of events in CI ITEM, Möbius, NRA
Generic	*Model entities:* High level	Dynamical	Study of cascading effects in

	Abstraction level	Theory	Applicable results and tools
cascading model, epidemiological models	Nodes (System Components) and links (structural, functional dependencies) *State Space:* Continuous, homogeneous High level, Complex networks	systems, causal networks Physics of complex systems, diffusion process in network	complex networks; the influence of the transient effects for the estimated cascade size, the role of exposure time for estimation of cascade size. Bespoke research models e.g. Java programming language; Touch-graph (open-source tool)
High and mid fidelity simulation of multiple infrastructures	The combines agents, discrete event simulation, 3D visualisation and scripting to investigate interdependencies and cascade effects within infrastructures. Also federated simulations.	Co-ordination and scenario models via agent models and associated scripting Various domain simulations (e.g. power grids, telco) often traffic or flow based	Provides direct examples of how infrastructures behave given a defined scenario. The most extensive examples in deployed systems. See INL CIMS tool. Research is on simulation standards and agent based approaches A number of generic agent based simulation frameworks are being developed (Cascadas) a well as muli-model frameworks such as Möbius, Ptolemy There is also specific infrastructure modelling approaches.
Domain simulations of single infrastructures	This is a mature field with all domains having a variety of models	Physics and flow based models	Behaviour of a specific infrastructure. Only partially covered in review.
Consequence models	Plume and blast models, crowd models, models of economic impact	Physics based models	*Not included in review*

Table 4: Research review - summary of models

4.4 Initial conclusions

From the stakeholder consultations and research review we can draw a number of conclusions:

State-of-the-art

- Certain modelling and simulation approaches can be deployed across a wide range of abstractions.
- There are impressive examples of detailed modelling and visualisation work as well as considerable experience and expertise in general simulation capabilities for domain or platform specific systems.

Off-line, soft real-time, hard real-time

- Most of the modelling work is off-line, but the capability to receive real-time data feeds exists. Real-time feeds include weather, GPS tracking (e.g. to identify closest police or emergency units).
- The use of interaction modelling off-line can increase the understanding and assist in protecting infrastructures against vulnerabilities and for defining efficient recovery strategies. However, the scenarios based approach can in practice only provide evidence for a relatively small number of scenarios. These need to be augmented with probabilistic assessments to provide an overall risk profile taking into account all types of events. There are clearly trade-offs here between levels of detail and fidelity.
- Can be used in slow moving situations to support decision making.
- There are some particular challenges in developing modelling capabilities that are trusted and accurate enough for real-time decision support.

Generalisation and lack of theories

- There are some general results from topological analyses that show, for example, the oft-cited "small world" properties of certain topologies. There are also some general models of cascade failures and epidemiological spreading that have been applied to infrastructure modelling. However, on the whole, there are very few theories and generic results.
- Generalising results from modelling and simulation to actual infrastructures is problematic. There is evidence from our consultations and from the literature that this is an area where details do really matter and while some general theories and results would be important they will need careful validation. For example, the work that investigates the level of fidelity needed in network dynamics to accurately predict cascades.

Maturity

- Much of the specific interdependency analysis is research based and uses bespoke software and has only been used by a small community—often the developers themselves. The work can be hard to repeat due to the sensitivity of results to the scenarios chosen, the parameters used in the modelling and lack of transparency of detailed assumptions.
- There are few, if any, comparative studies that would allow users, and by implication a "market", to decide on the required level of interdependency and infrastructure interaction modelling. What is appropriate for different threat levels, different mixes of infrastructures, scenarios and timescales is not known. The lack of evidence and the plethora of models is another indication of the immaturity of the field. Most models would have a low Technology Readiness Level (TRL).

Data

- There is also a requirement for data to support the infrastructure modelling process. Such data exists in certain domains; for example, telecommunication networks and electricity providers. Such data requires models of existing or

typical topologies as well as models of the assets that comprise those topologies.

- The requirement to model existing, in addition to fictional or proposed, infrastructures may require a data capture process that is currently available from a small number of specialist suppliers. Such data contributes to the synthetic natural environment required for certain types of infrastructure simulation. The need to trust the infrastructure analysis and models, the need to understand the caveats and uncertainties inherent in modelling, and the need for effective methods of risk communication all lead us to classify the integrated command and control requirements as ambitious.

Research practice and methodology

- There are a number of methodological and pragmatic issues in conducting convincing research in this area due to the scale and possible sensitivities of the work.
- There appears to be a gap between research and practice, and between the different research communities. There are a number of different communities (network "physics", complex systems, CIP etc.).
- There are difficulties with research methodology in this area. One of the difficulties is that of finding datasets and supporting scenarios to make realistic and convincing demonstrations. This can be due to cost, sensitivities and the need for interdisciplinary, particularly domain knowledge.

Business models and markets

The business model has to take into account the following:

- Currently a few customers and a market heavily dependent on and responsive to compelling advice from Government agencies
- Severe confidentiality and trust issues with infrastructure modelling
- Lack of maturity of interdependency modelling
- Some confusion as to who is responsible for the modelling
- Some innovation potential outside of the traditional CI modelling area

One view of the potential market is shown below in Figure 8. The market can be seen to be distinct segments dependent on the security sensitivity of the analysis. There are potential flows between the research and development and all the markets as well as between the different market segments. However, the measures and approaches required in each of these segments are likely to be different.

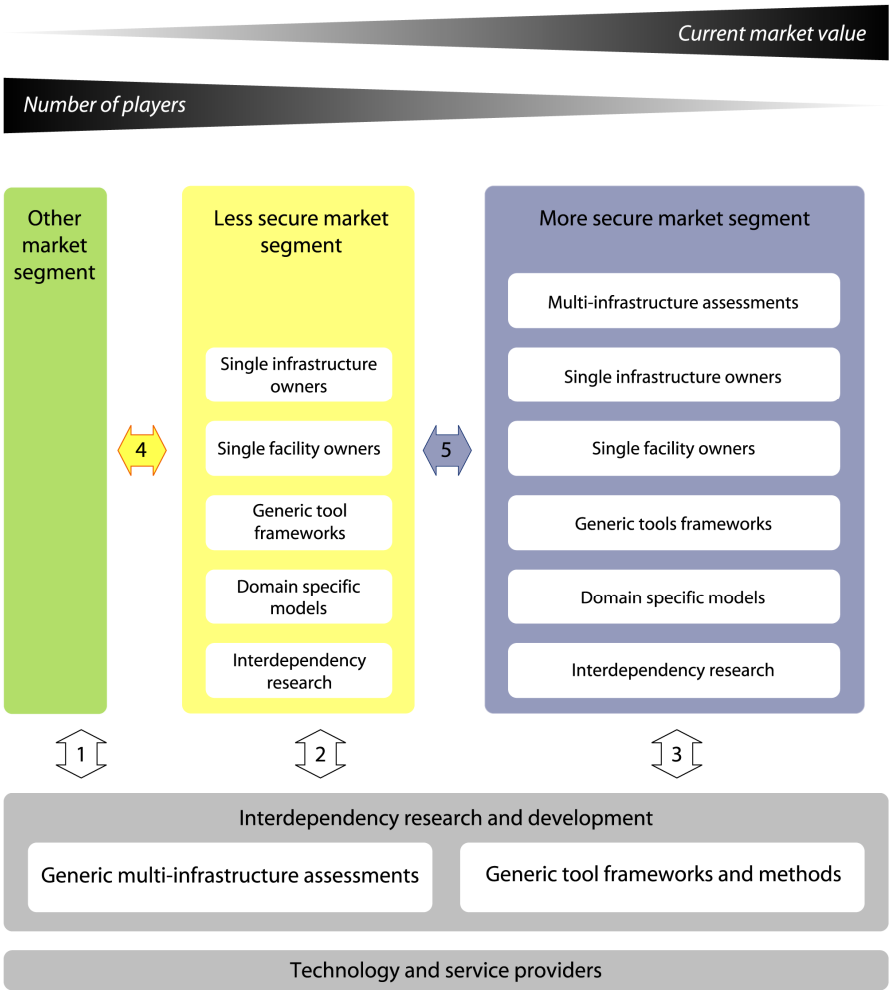

Figure 8: Market segmentation

Currently the work is dominated by the blue, secure, market with few players. The research and development tends to be poorly connected with the markets.

5 Recommendations and overall conclusions

5.1 Proposed outline strategy and conclusions

This study has consulted a wide range of CNI stakeholders from government, industry and academia who had interests in policy, research, risk and vulnerability analysis and innovation. We have undertaken a review of research [28] specific to understanding dependencies in infrastructures and other closely related aspects. This was followed by a gap analysis to identify whether further research and development might be required, and if so, what form it should take.

We have identified four main potential capabilities:

- To provide specialised security analysts with a means for the assessment of interactions and interdependencies.
- To provide off-line support for risk assessors both aggregators of risk (as at CCS) and also individual infrastructure owners to evaluate the impact of dependencies and interdependencies.

- To provide off-line support for risk assessors both aggregators of risk (as at CCS) and also individual infrastructure owners to evaluate the impact of dependencies and interdependencies during incidents (soft real-time).
- To provide real-time, decision support integrated command and control systems (hard real-time) that takes fully into account the impact of dependencies and interdependencies.

To address the required capabilities and gaps that we have identified we propose the following strategy.

5.1.1 Trial state-of-the-art and emerging research

Qualitative approaches. This task would develop and trial qualitative methods for modelling infrastructure interaction based on existing approaches for stakeholder groups as in CNIScan and also for CPNI assessors. The latter would require integration with CPNI processes and tools. The approach promises some short term gains.

Modelling approaches for off-line or soft real time. Develop and trial modelling of infrastructure interaction based on sufficiently detailed representations of the infrastructures, their environment and scenarios. The modelling would consider functional, topological and probabilistic approaches. The aim would be to develop clearer specification and assessment of benefits/costs. The trial should be sufficiently complex to enable scalability issues to be addressed and consider a number of different infrastructure mixes e.g.:

- Energy distribution (e.g. gas, electricity)
- Information infrastructures
- Soft intangible infrastructures (e.g. trust, confidence)

These could balance local detail of multi-infrastructures with the breadth of a single infrastructure system. The output of the exercise would be experience with the modelling approaches, assessment of costs/benefits and way forward and provide more clarity in current and future stakeholder requirements.

Real-time environment. Consider real time and synthetic environments separately as they have particular issues and challenges associated with them. Consider proposed future of decision support systems for key stakeholders and develop more detailed requirements to integrate interdependency approach.

5.1.2 Provide policy support and evidence base

Policy support. This would provide supporting analytical work on the justification and focus of the programme. It would develop further justification of benefits and propose improvements to incident reporting and analyses. It would analyse and integrate results of any modelling trials or experience reports.

Develop an interoperability approach. Develop an engineering approach with standards and guidelines to allow low barriers to specialising of any tools or methods (e.g. by use of standards, interoperabilities, published APIs). This should promote both innovation and also a more componentised approach.

Interoperability should cover behavioural models, topologies and associated data. Data costs can be significant and interoperability can provide an approach to amortising data costs across applications.

Define credible business models. Infrastructure and interdependency modelling has particularly close coupling to policy and to sensitive areas of risk assessment as well as the major role Government agencies have in encouraging and directing resilience related work. The type of eventual business model will be shaped by Government policy and action.

5.1.3 Knowledge transfer and co-ordination

Promote research base and connection to practice. This would involve enabling interaction (e.g. via knowledge transfer activities), addressing costs of research and methodologies and developing challenging research agenda. The agenda would initially be based on the review to be completed as part of this study but also in the light of the lessons learned in the trial of the qualitative and topologically detailed analysis approaches. Consider how to facilitate communication by disciplines and stakeholders and the advantages of a more formal risk communication framework and ontology.

In the interim, the sharing of interdependencies simulation expertise could be facilitated either by a public or industry sponsored forum, in a similar way to that in which the Opnet Defence Modellers Users Forum provides a platform for MoD to present requirements, examples and potential uses of telecommunications network simulation in defence to a group comprising a membership of industry providers and academia.

Within each of these threads there would be a need to consider both natural hazards and security vulnerabilities (e.g. by the use of different scenarios) and review each of the capabilities and gaps to ensure maximum coverage of issues.

6 Acknowledgements

We would like to thank the consultees who contributed to our study and namely the UK Civil Contingency Secretariat, the Australian CIPMA, Priority5, BT, BAe systems, Northrop Grumman, SE Validation, the European Commission's Joint Research Centre, DG INFSO Unit F5 'Trust and Security' and Unit A3 'Internet; Network and Information Security', Spearhead Technologies, ESRI UK, as well as the members of the SCADA and Control Systems Information Exchange who participated in our questionnaire survey.

We would also like to thank members of the UK CIIMWG who represent a range of key UK government departments.

The study has been funded by TSB, CPNI and EPSRC under contract NSIP/001/0001 – Feasibility Study on Interdependency Analysis. There has been partial financial support from our institutions and from the EU project IRRIIS (027568).

7 Glossary

ADM	Add-Drop Multiplexer
API	Application Programming Interface
ASPR	Office of the Assistant Secretary For Preparedness And Response
ARECI study	European Commission's Study on the Availability and Robustness of Electronic Communications Infrastructures
ASCE tool	Assurance and Safety Case Environment software Adelard, http://www.adelard.com/web/hnav/ASCE/index.html
BT	British Telecommunications
BAe Systems	British Aerospace Systems
Cascade effects and failures	Rapid propagation of the failure of a single component or node to multiple components/nodes *Also used in a specific sense to mean* the propagation of a failure of one infrastructure to one or multiple another infrastructures
CCS	Civil Contingency Secretariat, Home Office
Cetifs	CPNI, EPSRC, TSB Feasibility Study
CI	Critical Infrastructure A critical infrastructure (CI) consists of those physical and information technology facilities, networks, services and assets which, if disrupted or destroyed, have a serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of governments
CII	Critical Information Infrastructure
CIIMWG	Critical Information Infrastructure Modelling Working Group
CIP	Critical Infrastructure Protection
CIPMA	The Australian "Critical Infrastructure Protection, Modelling and Analysis" capability
CLIMB	Confidence Level In Model Behaviour
CNI	Critical National Infrastructure Those key assets of the national infrastructure (NI) the failure of loss of which could cause severe economic or social damage and/or large scale loss of life.
CNI Scan	CNI Shared Capability Advisory Network, see www.cniscan.org
CPNI	Centre for the Protection of National Infrastructure, see www.cpni.gov.uk
CSR	Centre for Software Reliability, City University London
DHS	Department for Homeland Security, USA
Dependency	Single direction dependencies of one infrastructure on another
DoD	Department of Defence, USA
DG INFSO	Directorate General "Information Society and Media"
DSTL	Defence Science and Technology Laboratory
ECI	European Critical Infrastructure Critical infrastructure located in EU Member States the disruption or destruction of which would have a significant impact on at least two Member States of the EU

EPCIP	European Programme for Critical Infrastructure Protection
EPSRC	Engineering and Physical Sciences Research Council
ESRI	Environmental Systems Research Institute
GIS	Geographical Information Systems
GPS	Global Positioning System
ICT	Information and Communication Technologies
II	Information Infrastructure
ISP	Internet Service Provider
ITEM	Reliability, Safety and Risk Assessment software tool ITEM, http://www.itemsoft.com/
Interdependency	Mutual dependencies among two infrastructures
IDRC	International Development Research Centre
IRRIIS	Integrated Risk Reduction of Information -based Infrastructure Systems
LLP	Limited Liability Partnership
MoD	Ministry of Defence
MODAF	UK Ministry of Defence Architecture Framework
NI	National Infrastructure The national infrastructure is the underlying framework of facilities, systems, sites and networks necessary for the functioning of the United Kingdom and the delivery of the essential services upon which the UK relies.
OECD	Organisation for Economic Co-operation and Development
PC	Personal Computer
SCADA	Supervisory Control and Data Acquisition
TRL	Technology Readiness Level
TNO	Toegepast Natuurwetenschappelijk Onderzoek, see www.tno.nl/
TSB	Technology Strategy Board, see www.innovateuk.org/

8 Bibliography

[1] "The Pitt Review: lessons learned from the 2007 floods", http://www.cabinetoffice.gov.uk/thepittreview.aspx

[2] Buncefield explosion official investigation website, http://www.buncefieldinvestigation.gov.uk/index.htm

[3] Business continuity case study: Northgate Information Solutions, http://www.businesscontinuityexpo.co.uk/page.cfm/Action=Exhib/ExhibID=0050/PageOption=ExhibLibraries_1/ProductID=11/OSite=0X0R0U_1331/t=m

[4] BBC news, "Mobile networks bear blast strain", http://news.bbc.co.uk/1/hi/technology/4659737.stm

[5] SC magazine, "Rare SCADA vulnerability discovered", http://www.scmagazineus.com/Rare-SCADA-vulnerability-discovered/article/109956/

[6] The Register, "BT fire disrupts emergency services", http://www.theregister.co.uk/2004/03/29/bt_fire_disrupts_emergency_services/

[7] Cabinet Office, Cm 6683, Transformational Government, Enabled by Technology, November 2005

[8] De Bandt O and Hartmann P, "Systemic Risk: A Survey", European Central Bank Working Paper NO. 35, November 2000

[9] European Commission, Availability And Robustness Of Electronic Communications Infrastructures, "The ARECI Study", Final Report, March 2007,ECSC – EC – EAEC, Brussels – Luxembourg 2007

[10] Rauscher K, Krock R and Runyon J, "Eight Ingredients of Communications Infrastructure: A Systematic and Comprehensive Framework for Enhancing Network Reliability and Security" Bell Labs Technical Journal, 2006, 11(3), 73-78

[11] Masera M, "Systems-of-systems: Interdependencies and Governance", IDRC, Davos 2008

[12] Simulation Interoperability Standards Organization, www.sisostds.org

[13] Cambridge Consultants, http://www.cambridgeconsultants.com/

[14] Common Validation, Verification and Accreditation Framework for Simulation (REVVA), http://www.revva.eu/

[15] Environmental Agency, "Case study: 2007 floods, tackling surface water flooding in Hull". http://www.environment-agency.gov.uk/commondata/acrobat/surfacewatercasestudy_1917504.pdf

[16] Bloomfield R and Gashi I, Evaluating the resilience and security of boundaryless, evolving socio-technical Systems of Systems, research report fro DSTL, Centre for Software Reliability 2008, http://www.csr.city.ac.uk/people/ilir.gashi/Papers/2008/DSTL/

[17] Hollnagel, E, Woods D, and Leveson N, eds, "Resilience engineering: concepts and precepts". Ashgate Publishing Company, 2006.

[18] BBC news, "Ulley reservoir dam burst fear", http://news.bbc.co.uk/1/hi/england/south_yorkshire/6239782.stm

[19] Spearhead Technologies, http://www.speartec.com/index.html

[20] Net Viz, http://www.netviz.co.uk/

[21] Chozos N, 2008, "Dependency aspects of an Emergency Department Safety Case", http://www2.warwick.ac.uk/fac/med/staff/sujan/ws_medsafe2008/programme/09_medsafe2008_nickchozos.pdf

[22] Carbon Footprint, www.carbonfootprint.com

[23] European Commission, "Critical Infrastructure Protection" projects information, cordis website: ftp://ftp.cordis.europa.eu/pub/fp7/ict/docs/security/fp7-ict-objective-1-7-cip-projects-synopsis-oct08-v2_en.pdf

[24] TNO report, "Literature Survey on effect-based operations: A PhD study on measuring effects and effectiveness of military operations", 2003, www.iwar.org.uk/rma/resources/ebo/Literature_survey_on_Effects-Based_Operations.pdf

[25] EU Project CI2RCO: D1 – Common Understanding of CI2RCO-Basics, 21 June, 2005

[26] Law A and Kelton W, "Simulation Modelling and Analysis". McGraw-Hill Science, USA, 1999.

[27] Department of Defence, "DoD Directive 5000.59: DoD Modelling and Simulation (M&S) Management," Aug. 2007; http://www.dtic.mil/whs/directives/corres/pdf/500059p.pdf

[28] Bloomfield R, Salako K, Wright D, Chozos N, Nobles P, "Infrastructure interdependency analysis: an introductory research review", Adelard document reference D/422/12101/4 issue 1, 2009, available for download at http://www.csr.city.ac.uk/projects/cetifs.html