2008

Visualisation of Critical Infrastructure Failure

W D. Wilde
Deakin University

M J. Warren
Deakin University

Originally published in the Proceedings of the 9th Australian Information Warfare and Security Conference, Edith Cowan University, Perth Western Australia, 1st December, 2008

Visualisation of Critical Infrastructure Failure

W.D.Wilde and M.J.Warren

School of Information Systems,
Faculty of Business and Law,
Deakin University,
Burwood, Victoria, Australia, 3217.

matthew.warren@deakin.edu.au and william.wilde@deakin.edu.au

Abstract

The paper explores the complexity of critical infrastructure and critical infrastructure failure (CIF), real life examples are used to discuss the complexity involved. The paper then discusses what Visualisation is and how Visualisation can be applied to a security situation, in particular critical infrastructure. The paper concludes by discussing the future direction of the research.

Keywords

Critical Infrastructure, critical infrastructure failure and Visualisation.

INTRODUCTION

This paper is directed at the potential impact of the critical infrastructure failure (CIF) upon the commercial organisation. It concentrates on a local perspective, which is much narrower than the general thrust of the relevant literature on a topic much more directed toward a national approach. Events such as the September 11, 2001 terrorist attack on World Trade Centre and the devastating 2004 Boxing Day tsunami which killed more than 225,000 people in Indonesia have brought the failure of critical infrastructure into acute focus. Both cause and effect of CIF are complex phenomena. A single cause may produce a cascade effect as when a computing failure causes an electrical breakdown which then causes a mass failure of human services throughout a broad geographical area. The effect may involve not just the failure of physical systems, examples of which include the power grid, water, transportation, and communications, but the socio-technical systems which depend upon them, for example, the financial network, food distribution and communications systems. Not least, the influence of human behaviour, regulatory agencies, and government must be factored in. As implied in this brief statement of the complexity of CIF, a hierarchy of "failure gravity" may be surmised from the firm's viewpoint. The firm's situation in an area devastated by flood is a very different prospect from a firm which has experienced a computing malfunction. But in both situations the firm is at risk although mitigation procedures may be implemented and potential consequences or losses assessed. Research in the area is minimal and research in the domain of Chief Executive Officer (CEO) awareness of the risk of CIF is at best elusive. To the CEO, a quantitative demonstration of risk is inscrutable; a visual presentation is potentially far more powerful.

Visualisation has been a topic of both academic research and commercial practice over the last decade, as a tool for analysis and education. This paper will explore some of the issues that relate to Visualisation and CIF.

CRITICAL INFRASTRUCTURE (CI)

In October 1997 the President's Commission on Critical Infrastructure Protection (PCCIP) in the US defined Critical Infrastructure as "*a network of independent, mostly privately-owned, man-made systems and processes that function collaboratively and synergistically to produce and distribute a continuous flow of essential goods and services*". (PCCIP, 1997) This definition was later expanded by the Critical Infrastructure Assurance Office

(CIAO) to include food/agriculture (production, storage, and distribution), space, numerous commodities (iron and steel, aluminium, finished goods, etc.), the health care industry, and the educational system. The CIAO defined infrastructure as "*the framework of interdependent networks and systems comprising identifiable industries, institutions (including people and procedures), and distribution capabilities that provide a reliable flow of products and services essential to the defense and economic security of the United States, the* smooth functioning of governments at all levels, and society as a whole" (CIAO, 1998).

In Australian terms the scope of critical infrastructure is classified as:

- Communications (Telecommunications (Phone, Fax, Internet, Cable, Satellites) and Electronic Mass Communications),
- Energy (Gas, Petroleum Fuels, Refineries, Pipelines, Electricity Generation and Transmission),
- Banking and Finance (Banking, Finance, and Trading Exchanges),
- Food Supply (Bulk Production, Storage, and Distribution),
- Emergency Services,
- Health (Hospitals, Public Health, and Research and Development Laboratories),
- Icons and Public Gatherings (Buildings (e.g., Sydney Opera House),
- Cultural, Sport, and Tourism),
- Transport (Air Traffic Control, Road, Sea, Rail and Inter-modal (Cargo Distribution Centers)),
- Utilities (Water, Waste Water, and Waste Management).Communications (Telecommunications (Phone, Fax, Internet, Cable, satellites) and Electronic Mass Communications)

(Abele-Wigert and Dunn, 2006)

Other nations have similar classifications. CI is classified from the perspective of national population survival in the event of major catastrophe. We have chosen to adopt the definition put forth by the U.S. Patriot Act, which identifies a critical infrastructure to be: systems and assets, whether physical or virtual, so vital to the United States *(or indeed any country*) that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters (Tolone et al., 2004). Under this definition, critical infrastructures may be organised according to the following sectors: agriculture, food, water, public health, emergency services, government, defense industrial base, information and telecommunications, energy, transportation, banking and finance, chemical industry and hazardous materials, postal and shipping, and national monuments and icons (Tolone et al., 2004).

Critical Infrastructure Interdependence

The cascading nature of infrastructure collapse is a major complicating factor in security analysis. The complexity of interdependence of critical infrastructures has been widely recognised and there have been a number of attempts to model its dynamics. The following figure (figure 1) illustrations discuss some of the approaches that have been attempted

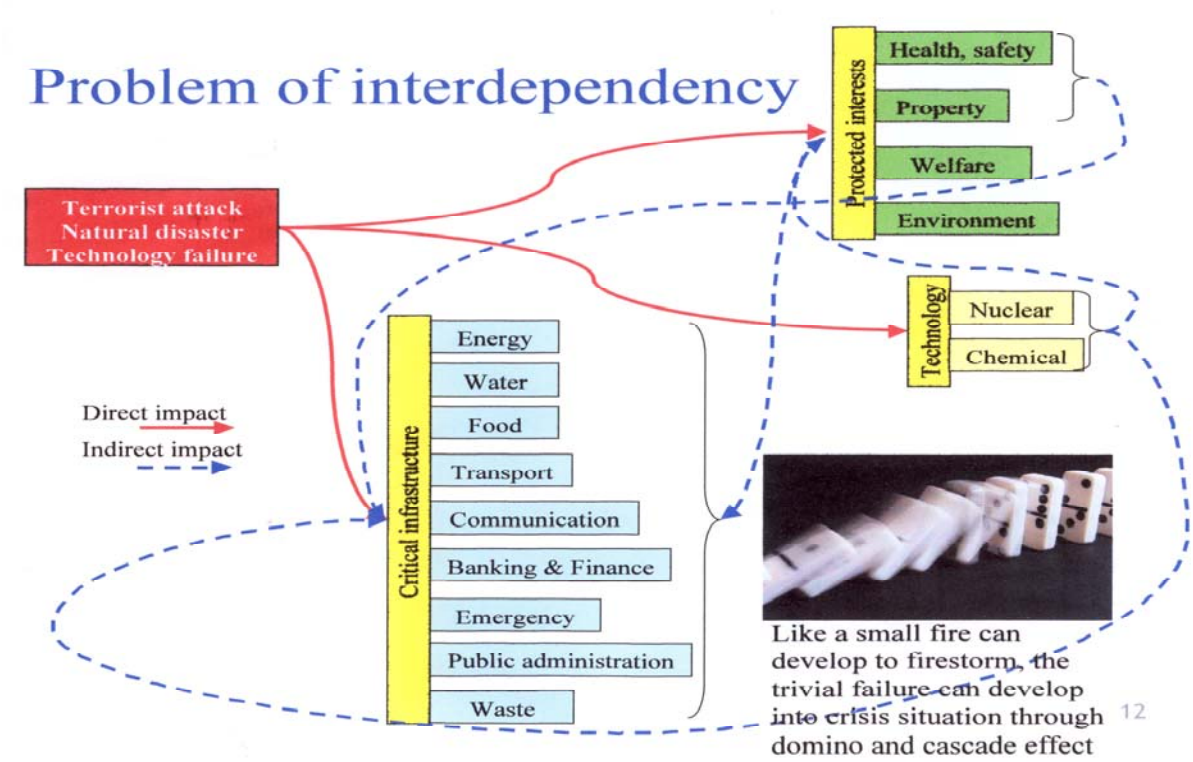

Figure 1 Critical Infrastructure Interdependency (Benes, 2007)

The nature of the problem is simply shown in Figure 1 by Benes (2007). The direct impact of a terrorist attack, natural disaster or technological failure on the electrical grid may then impact technology interests, such as a chemical plant, which may then cause severe social effects upon community health.

Pederson et al. (2006) contrived a simple illustration of the ties and dependencies of affected infrastructure in the single example of Hurricane Katrina as shown in Figure 2. "*The solid lines crossing sectors and connecting nodes, represent internal dependencies, while the dashed lines represent dependencies that also exist between different infrastructures*" (Pederson et al). The top grid, for example shows the connectivity of the affected electrical substations and which of these caused a particular sewage pumping station to fail. Similarly, a power failure in two electrical substations caused a communications breakdown

Rinaldi et al. (2001) in a much more detailed analysis have identified a number of principles. These have been constructed around a framework proposed by the PCCIP (1997) and comprise six dimensions (and shown by Figure 2):

- Infrastructure characteristics
- Type of failure
- State of operation
- Types of interdependencies
- Environment
- Coupling and response failure

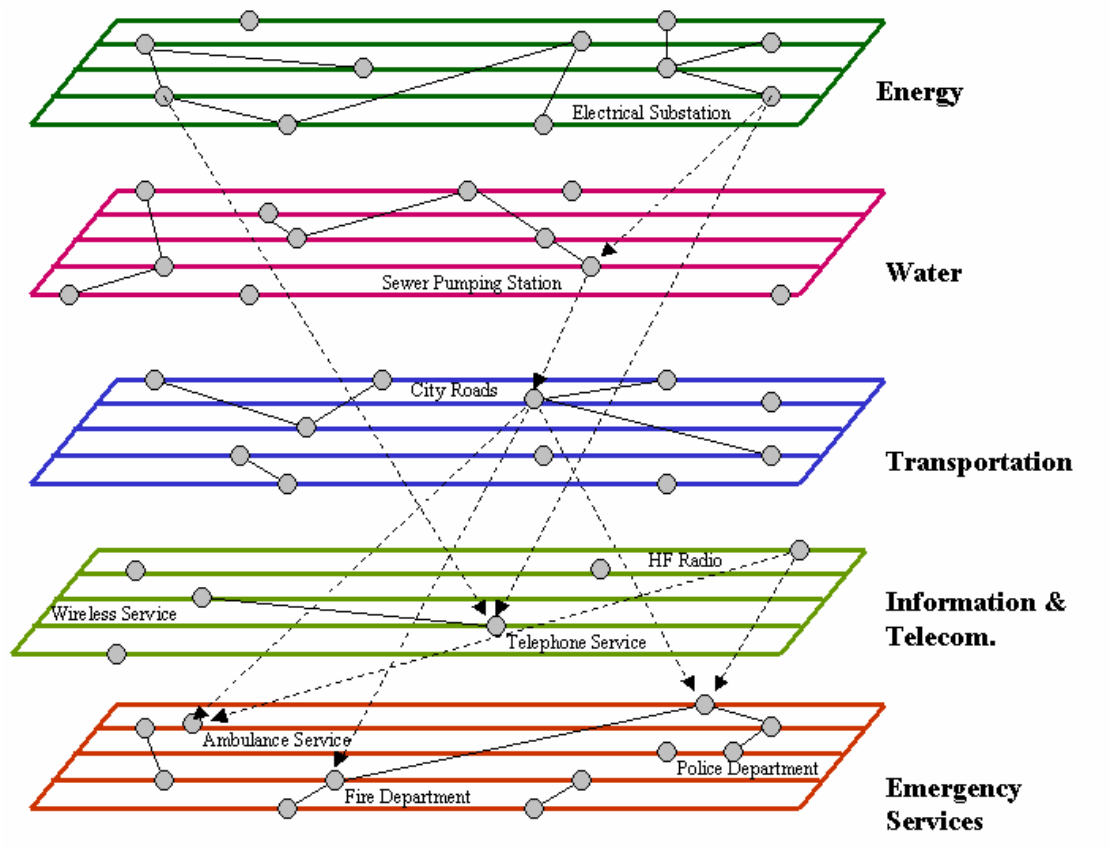

Figure 2 Critical Infrastructure Interdependency (Pederson et al., 2006)

An overriding principle of interdependency between two infrastructures may be unidirectional or bidirectional. In the first case, a pumping station supplying water to a community depends upon the electrical supply system but no dependency exists in the other direction. In the second case, a computer system and its electrical supply may be dependant upon each other. It is beyond the scope of this proposal to discuss the above framework in detail. However, discussion of a couple of the above dimensions will be instructive. The types of interdependencies, for example, consist of physical, cyber, logical and geographic. Physical interdependency is the direct linkage between two 'agents' such that the output of one is input to the other. Cyber interdependency is informational so that an infrastructure depends upon information from a computer as infrastructure to maintain its operation. Geographic interdependency is spatial and can occur when geographical proximity is such that the malfunction of one infrastructure can affect the operation of another, for example a coaxial cable attached to a collapsed bridge. Logical interdependency occurs in the absence of physical connections but where the functionality of one infrastructure, say a finance system, is dependant upon the integrity of another, say the computer system. A substantial insight into the protection of infrastructure is the dimension labelled Environment (see list above). This focuses upon the "*framework in which the owners and operators establish goals and objectives, construct value systems for defining and viewing their businesses, model and analyse their operations, and make decisions that affect infrastructure architectures and operations*" (Rinaldi et al. 2001; Sage, 1992). Economic and business opportunities and concerns, public policy, and legal and regulatory concerns are topics discussed as part of this dimension.

The conclusion reached by these authors is the scope of the challenge posed by the interdependence of the six dimensions of infrastructure and their individual attributes in planning for and mitigating against failure. Models of infrastructure have been built in many individual circumstances but simulation is a greater challenge. From the national viewpoint, a complete model of infrastructure would need to be built and this itself is an adaptive and evolving mechanism, the data needed on a real time basis to feed it and, importantly, its protection as the model itself would be an attractive target for cyber terrorists.

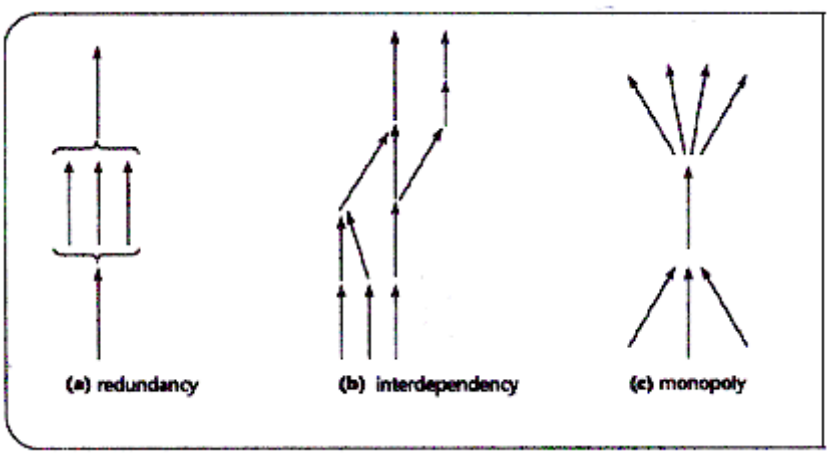

Figure 3 Economic Complexities (Borg, 2005)

Borg (2005) simply illustrates 3 types of interdependence as shown in Figure 3. If a path is redundant, that is two or more paths run in parallel as in (a), and one is compromised the total process will continue. The system is relatively robust. In (b), where one process depends upon many preceding processes, i.e., they are interdependent, which is the case in many assembly industries, and if a process which fits early into the system is compromised, many others will be thrown into disarray. This causes the well-known cascade effect. The final case (c), which is termed monopoly, is also a feature of many 'high tech' industries. A single company may provide under patent a single part which is crucial to the assembly. If compromised the total assembly process will halt for lack of this part.

Cyber Infrastructure

Cyber infrastructure in a modern economy is crucial and varied. It is arguable that the majority of major organisations are dependant to some extent on the Internet, but the Internet as a structure itself was built with survivability as a key ingredient. It is unlikely, therefore, that it will be destroyed. However, as more organisations establish websites and conduct business through the Internet, this connectivity to the external environment renders their web and application servers vulnerable. Further as Henderson (2007) states, technical advances increase this vulnerability. For example, "*Internet facing systems allow remote maintenance which saves money but opens systems to network-based attacks. Wireless architecture reduces network costs but opens internal network up to wireless attacks*" (Henderson, 2007).

The Internet is not only used for commerce. Increasingly, the SCADA (Supervisory Control And Data Acquisition) which refers to a large-scale, distributed measurement (and control) systems are Internet connected. Besides, in the US, 85% of CI is owned by the private sector and roughly 50% of CI sectors are controlled by SCADA systems (Henderson, 2007). Since this control technology is also vendor provided, any security strategy for process control must also be vendor built. SCADA systems are a good example of interdependency as discussed above. For, example, if a SCADA system which monitors and controls an electrical grid were to be compromised, this would prevent further control of the components of the grid as well as preventing the flow of information to other decision making processes that depend upon it. An emergency system, for example, might not receive data and be incapable of responding (Pederson et al, 2006).

In the cyber domain as in other CI domains it is important to identify the high risk areas of the existing infrastructure: the single points of failure and the recovery time limitations. But particularly for IT systems, it is important to identify the business critical applications and the systems that they run on as well as the areas of vulnerability within the environment (Shannon, 2002). SCADA systems are clearly a crucial candidate. These "threat vectors" comprise information about where a threat may originate and the assets it exposes to risk.

Henderson (2007) classifies threats to IT as structured and unstructured. Structured threats include:

- Bot-network operators,
- Criminal groups,
- Foreign intelligence services,
- Hackers,
- Insiders,
- Phishers,
- Spammers,
- Spyware/malware authors,

While unstructured threats include:

- Recreational hackers ("hacking for fun"),
- Malware (viruses and worms),
- Malicious insiders (disgruntled employees).

A more complete table of sources, threats and targets is found in Braggs et al, 2004 and is reproduced as table 1.

Sources	Threats	Targets
		Computer and peripheral
	Computer Theft	Communications equipment
	Intellectual property, theft or loss	Physical premises
	Confidential information exposure	Power, water, environmental control
Employees	Financial fraud	and communication facilities
Cleaning staff	Impersonation	Supplies and data storage media
Internet Attackers	Harassment	Operating systems
Contractors	Espionage	Computer Programs
Competitors	Denial of Service	Documentation
Terrorists	Software Malfunctions	Information and data
Accidents	Data deletion	Individual privacy
Weather	Data modification	Privacy of Intellectual property
	Data addition	E-mail
	Corruption of data integrity	Entities connected on the network
	Misuse of data	Telephone
	Loss of data	Voice Mail

	Human errors	Fax machines
	Physical hazards	Information
	Equipment malfunctions	Employee productivity
	Health and safety of people	

Table 1. IT Threats, sources and targets (Braggs et al, 2004)

THE ENTERPRISE PERSPECTIVE

From the viewpoint of the organisation there are basically two scenarios. The first concerns those phenomena which may cause critical infrastructure failure (CIF) but over which the organisation has no control. Floods, earthquakes, etc would fall into this category and for most organisations the probability of occurrence is very low. The second concerns those phenomena over which the organisation does have some control. This would include cyber failure where the probability of occurrence is greater than for natural phenomena. Regardless of the probability of occurrence, protection and mitigation procedures may be taken. However, in spite of investigating theoretical models of organisations no suitable structure around which a critical resource model may be built seems to exist. There are some, however, discussed below that provide some valuable clues to possible components.

Resource Based Advantage

The Resource Based Advantage model posited by Barney (1991) is basically about competitive advantage and suggests that organisations derive this from imperfectly inimitable or non-substitutable resources. Other commentators such as Duncan (1998) emphasise that this view is also true in the IT world where resources are particularly volatile, their value is heterogeneous across organisations and both of these serve to create an environment of uncertainty. It is the unobservable aspects of resources, namely organisational routines, management, knowledge, learning and the resultant capabilities (Prahalad and Hamel, 1990) developed by the organisation which are both inimitable and frequently non-understandable (Roy and Aubert, 2002) that yield competitive advantage. Duncan (1998) had already identified that, in an environment of extreme volatility, IT knowledge and expertise is a resource that an organisation has difficulty in acquiring and maintaining. But she also appreciated its value, in conjunction with a knowledge of the business and its environment, in recognising opportunities and implementing strategic initiatives. The value of this approach is that it identifies a subset of organisational resources and implies that it is the use of these resources, including IT expertise that constitutes CI and is subject to failure.

Porters Value Chain Analysis

Perhaps one the most widely known models of the organisation is Porter’s Value Chain Analysis which identifies a firm's core competencies and distinguishes those activities that drive competitive advantage. The model classifies the cost structure of an organisation into separate processes or functions and assumes that the cost drivers for each of these activities behave differently. Porter constructs a generic template consisting of five primary activities and four support activities shown as follows:

Primary activities:

1. Inbound logistics: materials handling, warehousing, inventory control, transportation;

2. Operations: machine operating, assembly, packaging, testing and maintenance;
3. Outbound logistics: order processing, warehousing, transportation and distribution;
4. Marketing and sales: advertising, promotion, selling, pricing, channel management;
5. Service: installation, servicing, spare part management;

Support activities:

6. Firm infrastructure: general management, planning, finance, legal, investor relations;
7. Human resource management: recruitment, education, promotion, reward systems;
8. Technology development: research & development, IT, product and process development;
9. Procurement: purchasing raw materials, lease properties, supplier contract negotiations.

The aggregation of these functions describes a complete organisation. Any loss of functionality would impact to some extent on the organisation and cause minimal or major financial loss. An interruption to the supply of materials, for example, would disrupt the production schedule and have serious financial implications whereas the organisation would suffer only minimally if a server malfunctioned and disrupted the education and training schedule. The Porter model includes service infrastructure (see 6 above) but, from the perspective of this research paper a physical infrastructure is also necessary. The housing of both the primary and support activities is clearly crucial as well as the equipment, principally computer equipment, which facilitates the activities.

The Input-Output Model

This is not strictly an organisational model but is included here because it provides a valuable perspective in quantifying the value of services to business functions (Rose, 2006). Figure 4 is a simple illustration of its underlying philosophy. For example, households funnel payments to markets for goods and services, which translate into revenue to the businesses that produce them. Businesses then make payments to the markets for factors of production, which generates household income.

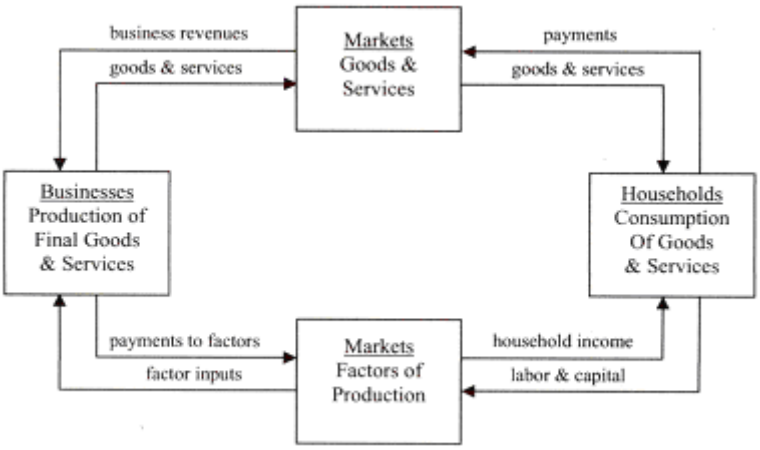

Figure 4 Basic Circular flow of the Economy (Rose, 2006)

The model is embellished in Figure 5 to include the intermediate means of production since businesses also need various types of raw and processed materials in addition to labour and capital to produce goods and services, as well as various services. Figure 5 also includes household activities to include the combining of market goods and services with time and household resources to yield "household production," i.e.,. cooked meals, recreation,

etc. And the requirement for infrastructure is acknowledged in the model in both business and household activities.

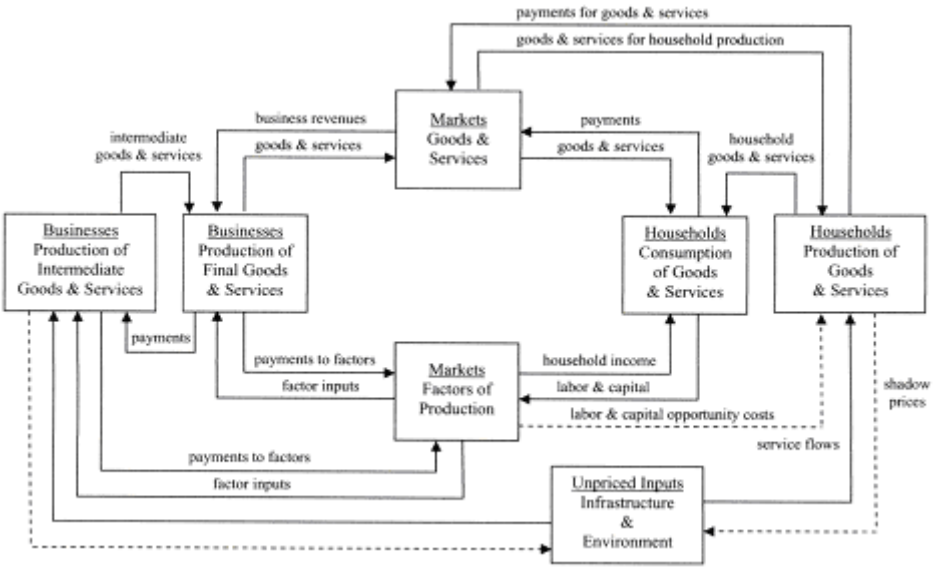

Figure 5 Expanded Circular flow of the Economy (Rose, 2006)

This model is incomplete without an accompanying matrix showing the interdependence of infrastructures. This is formed by mapping the sectors of the economy and infrastructures against each other. A simplistic example is shown in Figure 4. The LHS column row headings represent inputs and the column headings represent consumption. The contents of the cells are dollar values. So, for example, the figure 100 as shown matrix represents the value, say $100 million that the construction industry absorbs in electricity costs per annum (as shown by Table 2 and Table 2).

	Mining	Construction	Electric Utilities	Water	Manufacturing	Trade	Transportation	Communication	Information
Mining									
Construction									
Electric Utilities		$100m							
Water									
Manufacturing									
Trade									
Transportation									
Communication									

Information									

Table 2 Input/Output Table - General

	Warehouse	Manufacturing	Marketing	Distribution	Transportation	IT	Electric Utilities	Water	Communication
Warehouse									
Manufacturing									
Marketing									
Distribution									
Transportation									
IT		$1 m							
Electric Utilities									
Water									
Communication									

Table 3 Input/Output Table- Specific

Clearly this matrix has to be constructed to represent the entity under examination which is commonly the region. The value of the model is the identification of those key sectors of the regional economic structure and their quantification on dollar terms. From the organisational perspective it would need to be modified to represent economic sectors of the organisation and the infrastructural sectors that service them (See Figure 5 previously). Internal transfer value could also be quantified in this way although the degree of granularity would need to be considered. For example, it might be that the IT contribution the manufacturing is valued at $1 million but the separate value of electricity to each economic sector of the organisation might be too greater level of detail. The value of this model is that it identifies the dollar value (cost) of all functions within the organisation and the composition of that cost in a simple matrix form.

The Risk Calculation

This section demonstrates two simple risk calculations in common use depending upon the source of the threat. The first of these is more appropriate for an accidental, that is, non–intentional cause. In this case risk is a function of the probability of a threat modified by the vulnerability of the potential target of that threat and quantified by the financial damage that it would cause. Risk, therefore, is measured in financial terms, which is extremely meaningful to a CEO. So, for example, the threat of a earthquake to a business in Melbourne is very low, say .00000001. If, however, a earthquake were to occur, because the threat was so low, it would be economically infeasible that the organisation take any effective, expensive mitigating actions to reduce the threat even though the consequences in terms of damage might be very high.

Formula 1: Risk = Threat x Vulnerability x Consequence (Henderson, 2007)

Threat	Any person, circumstance or event with the potential to cause loss or damage.
Vulnerability	Any weakness that can be exploited by an adversary or through accident.
Consequence	The amount of loss or damage that can be expected from a successful attack.

Formula 2: Threat = Ability x Vulnerability x Intention (Benes, 2007**)**

The second calculation is a modification of the term 'threat' and is more suitable to the circumstances of intention. In this case, threat is not simply an 'act of God' but rather a function of deliberate strategy. This maybe represented by a terrorist or malicious employee targeting a specific area of critical infrastructure. For example, in 1999 one of the employees of the contractor involved in installing a new sewage pumping and treatment system for the council of Maroochy Shire in Queensland, Australia applied for employment with the council and was refused. (Byrnes, 2005) Between Jan 2000 and Apr 2000 the perpetrator released 264,000 gallons of raw sewage in 46 separate attacks into public waterways, which spilled into local parks as well as the grounds of a Hyatt Regency hotel. This was the first known use of a digital control system to attack public infrastructure. "*Software on his laptop identified him as "Pumping Station 4" and after suppressing alarms controlled 300 SCADA nodes*" the perpetrator was able to compromise vital infrastructure (Henderson, 2007).

Conceptually, therefore, each point of failure is subject to an analysis based upon the Formula 1 and 2 above. This implies that the basic variables are risk, mitigation and loss. The points of failure are multiple. Not only are the major public utilities involved, as seen in Figure 6, but the predominant position of computer in control situations, such as SCADA systems are truly critical in a situation where the major utilities have largely passed into private hands.

Management

The purpose of this section is to discuss the type of information that top management requires. There is an extensive literature about organisational management and management techniques (Drucker, 2006; Drucker and Senge, 2001, Pande et al, 2000; Mitzeburg, 1993, 2002; Argyris, 1987) and this has been expanding with the rapid adoption of electronic commerce and virtual organisations (Davidow and Malone, 1993; Tapscott, 1996) and globalisation (Ohmae, 2000). Many specific organisations have been examined in an attempt to discover organisational secrets of efficiency, eg. IBM (Moulton Reger, 2006), CISCO (Stauffer, (2000), Microsoft (Wallace, 1998) and many analyses have been made of organisational effectiveness (Peters and Waterman, 1984). On a broader scale, national strategies have also been discussed. Japan in particular has been the frequent focus of attention (Porter el al., 2000). But, from the point of view of this research proposal, effectiveness is to be pursued on a much smaller scale, that of managerial performance and particularly that of the CEO. The CEO has the responsibility of managing the entire organisation and so has the broadest span of control. The CEO is responsible for establishing policies, is future oriented, represents the organisation's interaction with its environment and takes responsibility for any consequences (Marakos, 2003). As such the information gathering needs of the CEO are of prime concern and must be both specialised and succinct. A popular and comprehensive method of determining the information needs centres around Critical Success Factors was developed by Rockart and Treacy (1982). Similarly a popular and (depending on its implementation) comprehensive method of presenting information to the CEO is the Executive Information System (EIS) which should provide (amongst other facilities) unstructured query support and graphical output (Marakos, 2003).

The concept of this study is the capacity to create an impression by the visualisation of leading executives regarding aspects of their organisational environment that are both varied and rarely aggregated. Critical infrastructure failure (CIF) is multi-faceted and has uncalculated potential impact. Thus, both the content and presentation of relevant information to the CEO are important. As already stated, in the context of this proposal the types of information are disparate. For example, the potential for and effects of deliberate attack or

accidental damage to a cyber system are complex and varied. However, these are of a different nature and scope than the disruption to a supply chain due to a chemical spill. But this is all CIF and may need to be presented to the CEO in a single illustration. Yet the forms of data are dissimilar. It may, for example, be desirable to inform a CEO of the number of attacks that have been attempted on a cyber system, how these have been mitigated, the cost of mitigation and the potential loss had mitigation been unsuccessful. This mainly falls into the realm of information visualisation since a data base of statistics may have been gathered for this purpose. On the other hand, the effects of a flood are in a different league. Not only is it probable that a flood has never occurred, but there will be no data base of statistics available. This could mean that a concept visualisation might be more effective. We will return to this topic in a later section after we have briefly covered the fundamentals of visualisation. We conclude this section by stating that risk, migration and prospective loss are the major factors of interest to the CEO in securing the organisation from critical infrastructure failure. Even though we recognise the complexity of interdependency in CIF as mentioned above (see Figure 6), for the purpose of this proposal, we ignore this since much of this is outside the CEO's control. The immediate organisational CI environment is of concern. For example, in the event of a power failure of the scope of the Auckland power failure of 1998 (NZMoED, 1998), power may be considered as a single point of failure and mitigation procedures such as the installation of private electricity facilities might have solved this problem for any specific organisation. Similar blackouts have been experienced in 2003 in Canada and in California in 2001 which testifies to the likelihood of such a failure.

VISUALISATION TECHNIQUES

The volume and complexity of knowledge and information in the modern era are such that unless a structure is superimposed upon it, it remains relatively meaningless. The requirement for 'information at your fingertips' precludes a requirement for time-consuming interpretation (Keller and Tergan, 2005). Indeed, the currently prevalent state of demand in the commercial domain is, firstly, that information to be readily accessible by users and, secondly, that the implications of complex information to be readily apparent. In this context, an appreciation that the power of visualisation is the foundation of the human cognition processing system is crucial. The "*power of a visualisation comes from the fact that it is possible to have a far more complex concept structure represented externally in a visual display than can be held in visual and verbal working memories*" (Ware, 2005, p29). Ware (2004) maintains that the cognition process comprises the human natural ability of pattern finding and Baddeley (1998) argues that visualisations draw upon both the visual and working memory systems. Consensus seems to have been adopted amongst researchers that drawing on the breadth of the human cognition systems serves to mitigate the limitations of working memory in both the capacity and duration of stored information.

Using visualisation as the interface between a computer-based information system and the flexible capabilities of human cognitive systems is an enormous enhancement over unaided cognition. Abstract relationships, particularly, are more easily processed by visualising links between elements (Cox, 1999) constituting a form of external cognition (Scaife and Rogers, 1996) resulting in what Rogers and Scaife (1997) refer to as 'computational offloading'. Presenting the audience with a diagram rather than a textual description allows it to exploit the rapid visual processing power of the human cognition system to make perceptual judgements rather than the laborious process of making logical ones (Paige and Simon, 1966). It may be, however, that visual clues may need to be augmented by verbal ones.

The complexities of the visual system are such that the topic to be visualised needs to be contextualised within the scope of the visual system's multiple capabilities and indeed of the sensory systems. Ebert (2005), for example, discusses 'perceptualisation' which includes several perceptual channels such as auditory, haptic and tactile, olfactory and kinesthesis. Ebert also discusses taking advantage of 'preattentive' visualisation, which involves low level parallel visual processing which requires no conscious cognitive effort.

Research into visualisation has broadly followed two avenues, the first being knowledge visualisation, adopted by the social scientists, and the second being information visualisation, adopted by the computer scientists (Keller and Tergan, 2005; Frank, H-J., Drosdol, J., 2005). Knowledge visualisation has an emphasis on conceptual knowledge and its visualisation potential. As such it focuses on the transformation of information to knowledge and is shown within a space characterised by knowledge elements and connections, so creating new meaning for eduction and decision making purposes. Mind maps and concept mapping are tools that are used to build a knowledge structure and to navigate around it. Information visualisation, by contrast, concerns the collection of data and its representation (i.e., objects, systems, events, processes, etc). in a visually spatial manner. It involves the representation of very lage and multivariate data sets generally for experts' use, and often does not provide user-friendly navigation or interfaces (Frank, H-J., Drosdol, J., 2005). Munzner (2000) considers that this knowledge/information distinction is debatable but tentatively defines information visualisation as hinging *"on finding a spatial mapping of data that is not inherently spatial"* and knowledge visualisation as using *"a spatial layout that is implicit in the data"*. Pasha (2004) discusses the problems of the visualisation of abstract data. "*With no natural mapping between data and graphical elements, the information designer is left with a considerable challenge to find a fit that that can maximise understanding and usability*" (p9).

We do not at this stage definitely select the domain into which this project falls since some data may be a natural fit and others may require a conceptual mapping. Our goal, by contrast, is much simpler to define. Roberts (2004) maintains that any visual system must have one of three goals: presentation, analysis or tactics. The first of these involves using the capacity of the human visual system to absorb immediately the implications of a situation or scenario. The conclusion is already known; basically this goal is about education. The second goal involves using a visual interface to find a conclusion from appropriately presented data. The third or tactical goal is to decide upon a course of action where time, or the lack of it, is of the essence. Military or stock market scenarios would be suitable contenders. In this proposal, consider that the main objective is to impact the CEO of the potential downside of CIF. If the project was restricted to data gathered as a result of attempted intrusions into an organisational cyber system, that data would have been organised into local data sets and would provide a simple mapping operation. If, however, the project incorporates the possible failure of power and communication systems, mapping will be a more complex function. Regardless, the focus is firmly on reader comprehensibility, enabled by information content and insight (Hanson et al, 1994). Clearly, in the simplest presentation case, diagrams will produce better performance than verbal representations, especially for more complex problems (Mayer, 1976*)*. In the simplest case, Munzer (2002) considers that "*graphs have a natural visual representation as nodes and connecting links arranged in space*" and so are, not surprisingly, pervasive. Even in problem solving, Carroll, Thomas and Malhotra (1980) *"found that spatial layouts of isomorphic design problems resulted in better performances and shorter solution times than temporal representations"* (quoted in Jonassen, 2005)

Importance of Visualisation in the Security Context

The purpose of this section is to emphasise the importance of visualisation in those areas which concern security. There are two principal reasons. Firstly, the detail of security is wide-ranging. The classification of infrastructure defined before (Abele-Wigert and Dunn, 2006) is a stark demonstration of the range of potential failures that may affect the performance of an organisation in the event of failure. In many cases organisations have no disaster plan or an untested one. In 2002 a VERITAS Disaster Recovery Survey suggested that 72% of all businesses have either no business continuity plan, never tested their plan, their plan failed when they tested it and only 18% of end user data is protected. (Shannon, 2002). Shannon also quotes Gartner (Roberta Witty, Donna Scott, 12 September 2001) who assert that "*Two out of five enterprises that experience a disaster go out of business within five years. Business continuity plans and disaster recovery services ensure continuing viability.*" A further quote from the Meta group states that "*CIOs who fail to conduct a business impact analysis risk over- committing or under-investing resources in disaster prevention and contingent recovery operations"*. The second reason that visualisation in the area of security is important is its complexity. The cascading effect of inter-dependent CIF is difficult to assess. Of the many areas of CI that organisations depend upon for normal

business functionality it may be argued that the most complex is the cyber infrastructure. This has also been thrown into prominence because of the high profile of hacking and computer software failure. It will be shown later in this proposal that the circumstances of cyber failure are probable and frequent and there are complex safeguards and mitigations. However, both the breadth and complexity of security concerns present problems in enlightening the CEO to the potential impact of disaster and might well be responsible for the dearth of business impact analysis and recovery plans. Many visualisations which have an analysis objective in complex areas are totally unsuitable for the CEO. But a principal objective of visualisation is the presentation of data. We argue that the only way to educate CEOs and other executives to the risk and consequences of CIF is an appropriate presentation of data that visualisation makes possible. In the ensuing sections we illustrate many visualisation possibilities and this proposal has the objective to explore them and develop both a suitable model for CIF and its appropriate visualisation.

CONCLUSION

The research described in the paper is part of a larger research project that is being conducted. The paper describes the complexity of Critical Infrastructure and failure and discuss the advantages that the visualisation technique could pose when be applied in this context.

The area of future research relates to the ways that visualisation can be used to best explain the complexity of understanding and how it can be used to understand Critical Infrastructure and especially its complexity. The aim next is to model a complex Critical Infrastructure scenario using visualisation techniques in order to allow a greater understanding of the situation.

REFERENCES

Abele-Wigert I., Dunn, M., (2006), “An Inventory of 20 National and 6 International Critical Information Infrastructure Protection Policies”, International CIIP Handbook 2006, Center for Security Studies, ETH Zurich, http://cipp.gmu.edu/archive/5_IntlCIIPHandbook_2006_Vol_I_Switz.pdf

Argyris, C., (1987), “Reasoning, action strategies, and defensive routines: The case of OD practitioners”, in *Research in organizational change and development* 1, Eds: Woodman, R. A., Pasmore, A.A., Greenwich: JAI Press.

Baddeley, A. D. (1998). *Human memory*, Boston: Allyn & Bacon.

Barney, J. B., (1991), “Firm resources and sustained competitive advantage”, Journal of Management, 17, pp. 99-120.

Benes, I, (2007), “Energy security and critical infrastructure resilience”, CITYPLAN, Prague, http://www.leonardo-energy.org/drupal/node/2300.

Borg, S., (2005), “Economically complex cyberattacks”, Security & Privacy Magazine, IEEE, 3(6), pp. 64 – 67.

Braggs, R., Rhodes-Ousley, M. Strassberg, K., (2004), “Network Security. A Complete Guide”, McGraw Hill, California

Carroll, J.M., Thomas, J.C., & Malhotra, A., (1980), “Presentation and representation in design problem solving”, British Journal of Psychology, 71, pp. 143-153.

CIAO, (1998), Presidential Decision Directive 63, Critical Infrastructure Assurance Office: http://www.ciao.gov.

Cox, R,. (1999), “Representation, construction, externalised cognition and individual differences”, Learning and Instruction”, 9, pp. 343-363.

Davidow, H. W. and Malone, M. S., (1993), "The virtual corporation", HarperBusiness, New York.

Drucker, P.F., (2006), “Managing the Non-profit Organization”, Collins.

Drucker, P.F., Senge, P.M., (2001), “Leading in a Time of Change: What it Will Take to Lead Tomorrow”, John Wiley and Son.

Ebert, D.S., (2005), “Extending Visualization, to Perceptualisation: The importance of perception in effective communication of information”, in The Visualization Handbook, Eds.: Hansen, CD. and Johnson, C.R., Elsevier.

Frank, H-J., Drosdol, J., (2005), “Information and Knowledge Visualization in Development and Use of a Management Information System (MIS) for DaimlerChrysler. A Visualized Dialogue and Participation Process” in *Knowledge and Information Visualization*, Eds: Tergan, S.-O., Keller, T., Springer-Verlag, Berlin Heidelberg, pp. 364 – 384, 2005.

Hanson, A.J., Munzner, T., Francis, G., (1994), “Interactive methods for visualizable geometry”, IEEE Computer, 27(7), pp. 73-83.

Henderson, M., (2007), “Protecting Critical Infrastructure from Cyber Attacks”, Department of Homeland Security, National Cyber Security Division, United States Computer Emergency Readiness Team, www.clcert.cl/seminario/US-CERT_Chile_2007-FINALv2.ppt.

Mayer, R.E. (1976). Comprehension as affected by structure of problem representation” in .Memory Cognition, 4(3), pp. 249-255.

Moulton Reger, S.J. (2006), “Can Two Rights Make a Wrong?: Insights from IBM's Tangible Culture Approach”, IBM Press

Munzner, T., (2000), “Interactive Visualization of Large Graphs and Networks”, PhD Dissertation.

NZMoED, (1998), “The Report of the Ministerial Inquiry into the Auckland Power Supply Failure”, Ministry of Economic Development, New Zealand, http://www.med.govt.nz/templates/Page____12136.aspx

Ohmae, K, (2000), “The Invisible Continent”, Nicholas Brealey, London

Pande, P.S., Neuman, R.P., Cavanagh, R.R., (2000), “The Six Sigma Way: How GE, Motorola, and and Other Top Companies are Honing Their Performance, McGraw-Hill

Paige, J.M., & Simon, H.A. (1966). Cognitive processes in solving algebra and word problems. In B. Kleinmuntz (Ed.), Problem solving: Research, method and theory (Chap. 3). New York, NY: Wiley.

Roberts, P., (2004), “Information visualization for stock marker tickets: Towards a new trading interface”, MSc Dissertation, MIT Sloan School of Management, http://lineplot.com/expertise/Thesis.pdf

PCCIP (President’s Commission on Critical Infrastructure Protection), (1997), “Critical Foundations: Protecting America’s Infrastructures”, http://www.ciao.gov

Pederson, P., Dudenhoeffer, D., Hartley, S., Permann, M. (2006), “Critical Infrastructure Interdependency Modeling. A Survey of U.S. and International Research, Idaho National Laboratory, INL/EXT-06-11464, https://www.pcsforum.org/library/files/1159904563-TSWG_INL_CIP_Tool_Survey_final.pdf

Peters, T.J. and Waterman Jr, R.H., (1984), “In Search of Excellence”, Harper and Row, Sydney

Porter, M.E., Takeuchi, H, Sakakibara, M., (2000), “Can Japan Compete?”, McMillan Press Ltd, London

Rinaldi, S.M., Peerenboom, J.P., Kelly, T.K, (2001), "Identifying, understanding, and analysing critical infrastructure interdependencies", IEEE Control Systems Magazine. December (2001), pp. 11-25

Rockart, J.F. and Treacy, M.E., (1982), "The CEO goes on-line", Harvard Business Review, 60(1), pp. 82-87

Rogers, Y., Scaife, M. (1997). External cognition. Retrieved February 10, 2005 from http://www.sv.cict.fr/cotcos/pjs/TheoreticalApproaches/ExtCogandRepr/ExtCogandReppaperRogers.htm#

Rose, A., (2006), "Regional models and data to analyze disaster mitigation and resilience", http://www.upenn.edu/penniur/pdf/events/PRESENTATIONS/Part%204/Regional-Final_11-9.pdf

Sage, A.P., (1992), Systems Engineering. New York: Wiley

Scaife, M., & Rogers, Y. (1996). External cognition: how do graphical representations work? Int. J. Human-Computer Studies, 45, 185-213.

Shannon Jr., H. F.(2002), "The Importance of Business Impact Analysis", VERITAS Software Corporation, www.nysforum.org/documents/ppt/bc_02/8-13VeritasBusiness%20Impact%20Analysis.ppt

Stauffer, D., (2000), "The CISCO Way", Capstone Publishing Ltd, Oxford

Tapscott, D., (1996), "The digital economy, promise and peril in the age of networked intelligence", McGraw-Hill, New York.

Tolone, W.J., Wilson, D., Raja, A., Xiang, W., Hao, H., Phelps, S., Johnson, .W., (2004). "Critical Infrastructure Integration Modelling and Simulation", in *Intelligence and Security Informatics*, Springer Berlin / Heidelberg, 3073, pp. 214-225.

Wallace, J., (1998), "Overdrive: Bill Gates and the Race to Control Cyberspace", John Wiley & Sons.

Ware, C. (2004) Information Visualization: Perception for Design (2nd Edition). San Francisco, CA: Morgan Kaufman.

Ware, C. (2005), "Visual Queries: The Foundation of Visual Thinking", in *Knowledge and Information Visualization*, Eds: Tergan, S.-O. Keller, T., Springer-Verlag, Berlin, pp. 27-35.

COPYRIGHT