Security Management: Modelling Critical Infrastructure

G. Pye[1] and M. J. Warren[2]

School of Information Systems
Deakin University, Australia,
[1]*Email: graeme@deakin.edu.au*
[2]*Email: mwarren@deakin.edu.au*

Abstract

Secure management of Australia's commercial critical infrastructure presents ongoing challenges to owners and the government. Currently a high-level information sharing collaboration between the government and business manages complex security issues, but critical infrastructure protection also lacks a scalable model exhibiting the overall structure of critical infrastructure at various levels, sectors and sub-sectors. This research builds on the work of Marasea and Warren (2003) to establish a representative model of Australia's critical infrastructure; discusses the boundaries between critical infrastructures, and considers the existence and potential influence of critical infrastructure relationships.

Keywords: Critical infrastructure protection and modelling.

Introduction

Modern commercial organisations regardless of size are now more so than ever reliant upon the continued provision of services delivered by the nation's critical infrastructure (CI) to conduct business and reliably service their customers. Furthermore, with the ease in which businesses can now access and utilise the services provided by CI and other non-critical infrastructure, business organisations may not necessarily be self-aware of their status or position within the nation's CI hierarchy.

CI is described as "those facilities and supply, information and communication networks that are essential for Australia's social and economic well-being and our national security" (AGD p1, 2004b) and it is through utilising some infrastructure services that businesses function and communicate electronically. Invariably, some business organisations taking advantage of such services may not necessarily realize, consider or understand the effects of their own imposition, obligation or adverse operations and security management obligations from their individual operational perspective within the CI system.

Notably in the 2004 Australian Computer Crime and Security Survey, participates where questioned, "Do you consider your organisation to be part of the critical national infrastructure?" (AusCERT, 2004, p.5). This question focused on the National Information Infrastructure (NII) as a subset of CI and related directly to the "infrastructure which comprises the electronic systems that underpin critical services such as telecommunications, transport and distribution, energy and utilities, and banking and finance" (TISN, 2004d, p1). What was notable about the response was that of the total respondents, 84 (35%) considered that their organisation was part of the critical NII, while 123 respondents (51%) did not and most significantly was that the remaining (equating to 14%) respondent organisations were unsure or unaware of their status with regard to their criticality and the NII.

ISSN 1445-3312 print/ISSN 1445-3347 online

Furthermore, this same question was included in the 2005 Australian Computer Crime and Security Survey, this time 32% of the total respondents regarded their organisation was part of the critical NII, while this time 52% believed their organisation was not part of the critical NII. Significantly, in the 2004 survey, 14% of respondents were not sure of their actual positioning or status concerning the critical NII and this level of uncertainty increased to 16% of respondents in the 2005 survey (AusCERT, 2005).

In view of these outcomes, the question arises: if a business organisation cannot identify their critically status and positioning within the NII, then by extension how do they identify their placement within the overall national CI hierarchy? This requires determination because organisational ignorance of their criticality status could potentially undermine the reliability and security of Australia's CI and business organisations of various sizes that utilise the subset NII services without necessarily having an appreciation of their risk liability and responsibility to the continued availability of CI services and the CI network at large. Additionally, other interconnected organisations and infrastructures within the CI network can suffer potential usability problems and security risks through the influence of functional dependency and interdependency relationships that exist between infrastructures. Thus, any adverse imposition on the continued availability of infrastructure services can by relation, threaten the very stability of the underlying information infrastructure systems within organisations, the NII subset and those infrastructures externally connected and represented by the national CI.

To address this organisational knowledge gap issue, it is proposed that the development of a scalable descriptive model encompassing Australia's overall CI will clearly establish boundaries between differing levels of infrastructure. This will enable any business organisation to determine their place within the national CI hierarchy, identify their security obligations and responsibilities, define their designated physical and digital boundaries and distinguish the specific connection points between differing infrastructure levels and subset infrastructures.

Additionally, after developing the CI model, it will also be necessary to investigate, define and interpret the potential influences of identified dependency relationships between critical infrastructures to confirm their existence, their type and likely influence upon and between related infrastructures. However initially, it is necessary to describe just what critical infrastructure is and review Australia's critical infrastructure protection program. This will assist in developing a descriptive model of the critical infrastructure that will both compliment and build upon the current security management paradigm of Australia's critical infrastructure protection and organisational security management.

Australia's Critical Infrastructure

Historically, the primary providers of infrastructure services in Australia was dispersed across the public sector at the Commonwealth, State and Local government levels where through the Australian federal system of government the provision responsibility for various infrastructure services is distributed from differing levels of government. For instance, the Commonwealth government is responsible for infrastructure services including: postal and telecommunications; and air transport services while the State governments are responsible for ports, rail, roads, gas and electricity, and water services. Local government also plays a role of infrastructure service provider across the state with the provision of local urban and rural infrastructure services such as water supply, sanitation and local road networks. The infrastructures fit into two broadly based groups, economic and social, where the economic

infrastructure relates to for example: the roads; railways; airports; water and waste water services; telecommunications; and power generation. While social infrastructures may include for example schools; health facilities; recreation facilities; housing; and law and order services (Smith, 2004).

Additionally, the private sector also plays a role in the delivery and provision of infrastructure services through ownership and under Public and Private Partnerships that broadly cover the financing and contracting obligations regarding the role of private sector infrastructure provision. Some of the key features of these partnerships include (Smith, 2004):

- Control over the core services is retained by government;
- Ensuring that the government is getting value for money with private sector bids;
- Safeguarding the public interest;
- The provision of services on a performance based contract; and
- An overarching partnership between the public and private sector.

Therefore, whether the infrastructures are economically or socially based, reside within the domain of the public or private sectors or exist as are partnership thereof, it is apparent that continued availability of some infrastructures and their services becomes critically strategic to the continued economic and social well-being of the nation. This is particularly relevant when considering that as much as 90% of the CI is under private sector ownership in some areas of Australia (TISN, 2004f).

According to Australia's national strategy, CI is defined as "those physical facilities, supply chains, information technologies and communication networks which, if destroyed, degraded or rendered unavailable for an extended period, would significantly impact upon the social or economic well-being of the nation or affect Australia's ability to conduct national defence and ensure national security" (AGD, 2004a, p1).

As a result, protecting Australia's critical infrastructure now requires a high level of cooperation between all levels of government and the private sector owners and operators. In response, the federal government has established and developed a policy for critical infrastructure protection management that focuses broadly on addressing the following strategies (Australian Government, 2004):

- Distinguishing critical infrastructures and ascertaining the areas risk;
- Aligning the strategies for reducing potential risk to critical infrastructure;
- Encouraging and developing effective partnerships with state and territory governments and the private sector;
- Advancing both domestic and international best practice for critical infrastructure protection.

Furthermore, the federal government have developed a short to medium term national strategy for CI protection that articulates an overarching statement of critical infrastructure protection principles and responsibilities that are applicable to all incumbent infrastructure stakeholders (TISN, 2004e).

Our National Critical Infrastructure Protection Strategy

The Australian national strategy for critical infrastructure protection was formally adopted in March 2004 (Booth, 2004) and is based on a coordinated and cooperative 'committee-like' *[sic]* approach to information sharing in relation to the protection of critical infrastructure. This requires the proactive engagement of infrastructure owners, operators, regulators, professional bodies and representative industry bodies, all levels of government and the public. To this end, the strategy outlines nine guiding principles central to the protection of Australia's critical infrastructure (AGD, 2004a):

1. Minimising risk to public health, safety and confidence, maintain economic security and international competitiveness and ensure continuity of government and its services;
2. Identify critical infrastructures and identify potential vulnerabilities, interdependencies and prepare and protect them from hazards;
3. Utilise appropriate risk management techniques to establish relative criticality, level of protection required, priority for resource allocation and the application of effective mitigation strategies for business continuity;
4. The onus for the management of risk within physical facilities, supply chains, information technologies and communication networks resides with the owners and operators;
5. Critical infrastructure protection should be considered from the 'all hazards approach' *[sic]* that accommodates interdependencies between business, sectors, jurisdictions and government agencies;
6. A consistent and cooperative partnership between the owners and operators of critical infrastructure and the government is paramount to/for effective protection;
7. Effective protection and better risk management will be further enhanced by effective sharing of information relating to threats and vulnerabilities between government and the owners and operators;
8. Information of any national security threats to critical infrastructure, must be handled carefully and responsibly to avoid creating undue concern within the domestic community, tourists and overseas investors;
9. Encourage further research and analysis of risk mitigation strategies tailored to Australia's unique critical infrastructure context.

These nine principles provide a broad commonality of understanding regarding risk management and protective obligations between critical infrastructure stakeholders and Australia's national strategy. Furthermore, they underpin the national strategy by encouraging the CI owners, operators to participate within the Trusted Information Sharing Network (TISN) set up by the federal government as a confluence mechanism to share, and exchange relevant information provided by all stakeholders and national security services. This information pertains to important matters such as business continuity, incident and consequence management, information system attacks and vulnerabilities, electronic crime, protection of key sites from attack or sabotage, chemical, biological and radiological threats to water and food supplies and the identification and protection of offshore and maritime assets. By following the nine guiding principles outlined in the national strategy infrastructure stakeholders can negate or reduce the potential effect of an incident/s adversely influencing the functionality and availability of CI services. Therefore, the principle focus of the national strategy is on the medium to long term strategic CI protection requirements that are integral to providing common guiding perspective to addressing identified risks and emergent incidents that require an immediate national response (AGD, 2004b).

This is particularly relevant when considering the situational environment that uniquely distinguishes CI from the Australian perspective, such as:

- Australia is a large island continent;
- Minimal sharing or reliance on external infrastructures and services located or provided from outside the national border;
- CI is spread over a large geographic areas with limited populations in remote regions of the country;
- Largely immune from foreign critical infrastructure incidents, although this is not entirely the case from a cyber perspective;
- Due to remoteness, there is potential for early warnings regarding externally based incidents and perhaps isolation from the effects thereof, but Australia is not itself immune from the effects of externally originating incidents and nor can it be expected to totally contain internally based incidents.

This is particularly applicable to an expansive area across a number of differing economic and social sectors that critical infrastructure supports, such as banking and finance, transport and distribution, energy supplies, utilities, health, food supply and communication, as well as government services and national icons (AGD, 2004a). The following list from the National Counter-Terrorism Committee (NCTC), which is a high-level government committee advising on security, identifies these sectors and sub sectors as representing Australia's critical infrastructure (NCTC, 2004):

- **Energy Sector:** Gas, Petroleum Fuels, Electricity Generation and Transmission.
- **Utilities Sector:** Water, Waste Water and Waste Management.
- **Transport Sector:** Air, Road, Sea, Rail and Inter-modal (cargo distribution centres).
- **Communications Sector:** Telecommunications (phone, fax, Internet, cable satellites), Electronic Mass Communication and Postal Services.
- **Health Sector:** Hospitals, Public Health and Research and Development Laboratories.
- **Food Supply Sector:** Bulk Production, Storage and Distribution.
- **Finance Sector:** Banking, Insurance, and Trading Exchanges.
- **Government Services Sector:** Defence and Intelligence Facilities, House of Parliament, Key Government Departments, Foreign Missions, Key residences, Emergency Services (Police, Fire, Ambulance and others) and Nuclear Facilities.
- **National Icons Sector:** Buildings, Cultural, Sport and Tourism.
- **Essential Manufacturing Sector:** Defence Industry, Heavy Industry and Chemicals.

While some sectors are clearly within the defined scope of critical infrastructure, the federal government maintains that connective networks or supply chains that deliver essential products and services are strategic parts of the overall critical infrastructure. This is due to their relational dependence or interdependence on the availability of other infrastructure sectors to provide continuity of service supply and therefore consequently is also affording some dependency overlap between CI sectors and sub-sectors (AGD, 2004a).

Therefore, to manage CI from the Australian perspective the government, through the Trusted Information Sharing Network (TISN) structure, can coordinate and manage security information sharing and the protection of the identified infrastructures that is critical to Australia's continuing social and economic well-being (AGD, 2004b).

Trusted Information Sharing Network (TISN)

The TISN provides a forum to encourage the development of information sharing partnerships between business and the federal government on significant security issues (AGD, 2004a). As Walker (2004) indicates, the TISN web portal provides a direct link between Australian Security Intelligence Organisation (ASIO) and business leaders to exchange information and coordinate existing strategies, plans and procedures that necessitate the prevention, readiness, responsiveness and recovery systems in the event of adverse incidents threatening and affecting critical infrastructure. The following areas of specialisation are utilised to provide the information, expertise and support necessary to deliver, combat and manage adverse critical infrastructure incidents in the Australian context (TISN, 2004a):

- Law enforcement and crime prevention;
- Counter terrorism;
- National security and defence;
- Emergency management and the dissemination of information;
- Business continuity planning;
- Protective security (physical, personnel and procedural);
- E-security;
- Natural disaster planning and preparedness;
- Risk management;
- Professional networking; and
- Market regulation, planning and infrastructure development.

The TISN is a hierarchical management structure which consists of a number of advisory groups that all interact and 'network' *[sic]* together under the auspice of the Australian Government's Attorney-General's Department (AGD). The Critical Infrastructure Advisory Council (CIAC) oversees the Infrastructure Assurance Advisory Groups (IAAGs) and Expert Advisory Groups and provides medium to long-term advice to the AGD on the national approach to critical infrastructure protection and deliberates on emergent issues, particularly any interdependence issues raised by the groups within the TISN network. The AGD chairs the CIAC council that consists of representatives from critical infrastructure business sectors, relevant federal, state and territory government agencies and the NCTC (AGD, 2004a). The IAAGs represent the business sector groupings created as a forum for respective owners and operators of critical infrastructure to meet, discuss and share information on common threats and vulnerabilities as well as appropriate information on strategies and measures to mitigate risk within their respective business sector group (Booth, 2003).

Under this consultative and information sharing regime, critical infrastructure stakeholders are expected to develop and maintain implementation plans for critical infrastructure protection that is aligned to the national strategy and are obligated with the following provision responsibilities (TISN, 2004b):

- Asset security;
- Risk management and planning processes;
- Regular reviews of risk management and planning processes;
- Incident reports and reporting suspicious activity to police;
- Development and regular revision of business continuity plans;
- Involvement in exercises that test business plans in place, as conducted by government authorities.

According to Walker (2004), the development of an information sharing approach to the management of the security of Australia's national critical infrastructure only became operational in early 2005 and the TISN continues to expand. Furthermore, according to Fleckner (2004) this supports the premise that the increase in private sector ownership of critical infrastructure necessitates that the management and protection of these essential services and utilities has to have a federal government led and coordinated approach that the TISN now represents.

With this stance taken by the federal government, the onus squarely rests with the individual owners and operators of critical infrastructure to implement effective IT security regimes for NII protection and physical security, which deliver best practice asset security and meets the aspirations of the TISN's critical infrastructure protection program (Walker, 2004).

The Foundation of Australia's CI Model

The critical infrastructure security management system within Australia is focused at the high-level end of the management spectrum and is based on information sharing structure where specific groups will get together to discuss and share their relevant security issues. The TISN structure has merit at this level of application, but needs to deliver further information that would assist businesses in making critical self-judgements about their specific place within Australia's critical infrastructure hierarchy.

While the current TISN structure is a high-level hierarchy, the various IAAG's consisting of the particular corporate businesses or organisations that have to coordinate with each other and share the information passed down represents a sectionalised structure that fails to represent an overall elemental view of Australia's critical infrastructure. Therefore, to resolve the ambiguous situation the authors propose developing a model representing and depicting the structure of Australia's critical infrastructure and its elemental components which will enable organisations to critically identify and evaluate their place within the CI structure, thus allowing them to determine their likely security obligations and criticality, with regard to the overall national critical infrastructure hierarchy.

The basis of Australia's critical infrastructure model is to develop a model combining a number of current critical infrastructure viewpoints expressed in the literature. The first is the critical infrastructure sectors and sub-sectors, which clearly identifies the various infrastructure types regarded as critical to the national interest by the NCTC (2004). The second is the TISN structure that presents a high-level 'committee-like' *[sic]* view of how the various infrastructure groups, representing individual infrastructures network together.

While CI management models of other nations do exist, this paper is representative of the current Australian government's strategy and therefore presents the current CI contextual representation from the Australian perspective that incorporates the government's CI management strategy.

It is also important to recognise and incorporate the characteristics that organisational networks and their infrastructures can span across physical and designated borders, differing regulatory jurisdictions, while also engaged at differing levels within the context of Australia's critical infrastructure. Therefore commercial organisations should be able to locate their place within the overall model of Australia's critical infrastructure to recognise 'duty of care' *[sic]* and governance issues, while also recognising where security responsibility and

obligation boundaries exist, as aligned with the nine critical infrastructure management principles enumerated previously.

Modelling Australia's Critical Infrastructure

This model of Australia's critical infrastructure incorporates differing levels of infrastructure that includes the various sectors and sub-sector infrastructures pertaining to each level within the model. This approach will clearly determine the general physical boundaries between levels and allow further extrapolation to identify the precise connection points between levels that will further clarify and delineate infrastructure ownership; governance obligations; duty of care; maintenance; security management, and protection responsibilities.

Additionally, a scalable model representation will further assist in the identification of dependency and interdependency inter-relationships between infrastructure levels, sectors and their sub-sectors from the individual user at the personal level through to the global level.

Sectionalising Critical Infrastructure into Levels

The critical infrastructure model will consist of five broad based infrastructure levels that clearly define the physical boundaries between each level. Within each infrastructure, level will be the individual critical infrastructure sectors and sub-sectors as listed previously. The following list indicates the various infrastructure level categories:

- Global – infrastructure that extends across international boundaries or is infrastructure located within another sovereign nation;
- National – infrastructure that extends across state boundaries, but remains within the national borders;
- State – infrastructure that is confined within the border boundaries of the respective Australian state's jurisdiction;
- Corporate – infrastructure that is confined within the property boundaries of the particular corporate or business entity;
- Personal – infrastructure that is not the property of any supply authority infrastructure or within the corporate jurisdiction, but is located within a domestic situation.

Upon sectionalising of Australia's critical infrastructure into the previously defined levels, as modelled in Figure 1, this now illustrates generally definable and recognised boundaries between the various critical infrastructure levels. Although it is recognised that infrastructures, their ownership, and management thereof can exist and overlap across the established sectors and sub-sectors of the model produced, it is important to consider that the model now represents the possible categories within which CI can now be classified and indicates the particular infrastructure's positioning, possible criticality and dependency relationships with other CI's,

Furthermore, because of the model sectionalisation, the issue of potential dependency inter-relationships existing within the infrastructure model needs further consideration to identify the differing types of infrastructure dependencies and interdependencies that add further complexity within the elemental scope of the critical infrastructure model. The existence of these infrastructure dependency relationships requires serious consideration due to the potentially expansive implications and possible functional impact they could inflict upon the availability of critical infrastructure services. Therefore, it is desirable to develop an approach to map and simply represent dependency and interdependency relationships that exist within the national critical infrastructure, thereby delivering further underpinning structural

information support that further compliments the TISN high-level concept, as it currently exists.

Critical Infrastructure Dependence and Interdependence

To understand clearly the implications and meaning of the terms dependence and interdependence within the concept of critical infrastructure, we need to define clearly an understanding of the meaning and use of these terms. The term dependence is defined by the Oxford English Dictionary (Pearsall, 1998, p.495) as "the state of relying on or being controlled by someone or something else", while the term interdependence as defined by the Oxford English Dictionary (Pearsall, 1998, p.951) as "(of two or more people or things) dependent on each other".

The NCTC (2004) acknowledges that dependencies do exist and that most critical infrastructure operators are dependent to a varying extent on the uninterrupted supply of electricity, water, fuel, shared information systems and emergency services. Furthermore, infrastructure services such as electricity, transport, and telecommunications are additionally dependent on the continued security of supply.

Additionally, within the subject literature confusion of meaning and inter-changeability of terms exists in the descriptive use of the terms dependence and interdependence. The authors have proposed here, an attempt to clearly define and delineate the difference between the applied terms of dependency and interdependency.

Therefore, a critical infrastructure dependency is a one-way reliance or influence of one critical infrastructure level and/or its infrastructure sectors has on another critical infrastructure level and/or its sectors for continuity of supply and delivery of services.

Critical Infrastructure Dependency Types

The authors propose that any type of critical infrastructure dependency within the model will be categorised as being one of the following three descriptive types:

- TCID (Total Critical Infrastructure Dependency) are those critical infrastructure dependencies that exist across all infrastructure levels modelled;
- MCID (Multiple Critical Infrastructure Dependency) are those critical infrastructure dependencies that exist across three or more infrastructure levels, but not all;
- BCID (Bridging Critical Infrastructure Dependency) are those critical infrastructure dependencies that exist between only two critical infrastructures levels.

In addition, the dependency relationship based on the premise that there exists reliance or influence from one infrastructure level or sector on another, or multiple thereof, for delivery of service is to be deemed a heavily biased or one–sided relationship. If this relationship was mutually reliant and the dependency influence distributed with greater equity between the infrastructures, then it is an interdependency relationship. It must also be considered that these relationships can also exist and exert influence on critical infrastructure not only as shown in the model, but also at the elemental level that exists between infrastructures and can overlap across levels, sectors and sub-sectors.

The Critical Infrastructure Model

	Global Level Infrastructure
Sectors	**Sub-Sectors**
Communications	Telecommunications (Phone, Fax, Internet, Cables, Satellites), Electronic Mass Communication
	Postal Services
Government Services	Defence and Intelligence Facilities, Foreign Missions
Transport	Air (inter-modal distribution centres), Sea (inter-modal distribution centres)
	Gas and Fuel Supplies (oil and Gas Fields)

	National Level Infrastructure
Sectors	**Sub-Sectors**
Communications	Postal Services
Energy	Interstate Transmission and Supply (Electricity, Gas, Petroleum Fuels)
Federal Government Services	Key Residences, Nuclear Facilities, Essential Government Departments, Houses of Parliament
National Icons	Buildings, Cultural, Sport and Tourism
Transport	National Roads (Highways), National Rail

	State Level Infrastructure
Sectors	**Sub-Sectors**
Energy	Generation, Processing and transmission (Electricity, Gas, Petroleum Fuels
Transport	State Roads, Bridges, Tunnels, State Rail
Health	Hospitals, Public Health, research and Development Laboratories
State Government Services	Emergency Services (Police, Fire, Ambulance), State Houses of Parliament

	Corporate Level Infrastructure
Sectors	**Sub-Sectors**
Essential Manufacturing	Defence Industry, Heavy Industry and Chemicals, SCADA Systems
Finance	Banking, Insurance and Trading Exchanges
Food Supply	Bulk Production, Storage and Distribution, Processing, Cooperating Supply Chains
Local Government Services	Urban Councils and Shire Councils
Utilities	Water, Waste Water and Waste Management
Corporate Infrastructure	Electricity, Water, Gas; SME Networks; Corporate Networks

	Personal Level Infrastructure
Sectors	**Sub-Sectors**
Domestic Infrastructure	Electricity, Water, Gas
	Home PC Networks

TCID: NII (Telecoms), Electricity, Information Technology (IT).

MCID: Defined as those dependencies that impinge across three or more critical infrastructures, but not all.

BCID: Defined as those dependencies that impinge between only two critical infrastructures.

Figure 1: Critical Infrastructure Model

Therefore, through the development of the model of Australia's critical infrastructure as shown in Figure 1, this further compliments both the TISN (2004a) structure and the NCTC (2004) findings by clearly illustrating infrastructure levels, sectors and sub-sectors within a defined structure. Hence, corporate organisations will be able to utilise this to determine and identify whether their infrastructure is either critical or non-critical.

Additionally within the model is represented the TCID dependency relationship that exists across the entire model and represents the dependency that Australia's critical infrastructure has on the continued supply of electricity, telecommunications and information technology infrastructure as determined by the research of Marasea and Warren (2003).

However, the specific boundaries between the infrastructure levels within the model at the lower levels is still general and requires further investigation to more specifically identify and reveal the actual connection point between infrastructure levels, sectors and sub-sectors and to establish where infrastructure responsibility begins and ends.

Critical Infrastructure Boundaries

The physical boundaries between the infrastructure levels in the critical infrastructure model at the global, national and state levels are clearly established and recognised. However, the physical boundaries of the state, corporate and personal infrastructure levels have been generalised to reflect the physical infrastructure situated within property boundaries. This demarcation point is not yet specific enough to represent the actual nexus point boundaries between the state, corporate and personnel infrastructure levels.

Physical Boundaries

The physical infrastructure nexus point boundary between the state, corporate and personal level is the actual connection point between the infrastructure service provider or distributor and the point of attachment onto the particular property's infrastructure, rather than at the prescribed property boundary.

The precise nexus point of demarcation identified in the electricity supply industry's Australia and New Zealand Standard Wiring Rules AS/NZS 3000 (Standards Australia, 2000), is the Point Of Attachment (POA), which is the specific connection point where the distributor's supply infrastructure is terminated onto the consumer's building and therefore corporate or personal infrastructure. For such utility services as water and gas supply infrastructure, in this situation the POA would be the supply side of the metering point situated on the property, as shown in Figure 2.

Likewise, in the case of telecommunications infrastructure a similar point of demarcation can be defined and applied, although, the terminology used in the relevant Australian Standard for the Installation Requirements for Customer Cabling (Wiring Rules) AS/ACIF S009:2001 (Standards Australia, 2001), refers to the Main Distribution Frame (MDF) as the point of attachment. Therefore, once again the principle of a commonly identified connection point separates the service provider or supply authority infrastructure and the corporate or personal consumer infrastructure, as depicted in Figure 2.

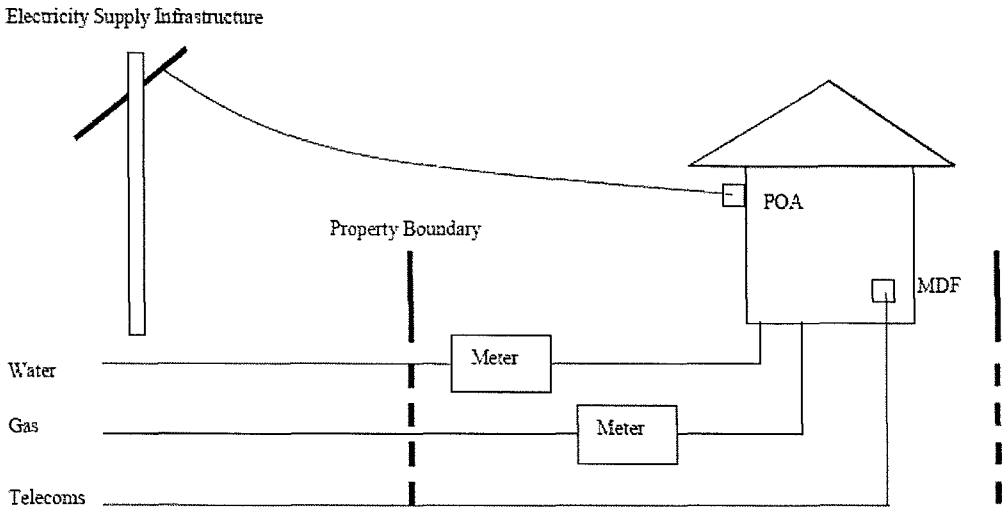

Figure 2: Physical Infrastructure Demarcation Boundaries

Hence, the specific nexus points between infrastructure ownership boundaries clearly establishes the recognised points of interconnection between the respective state, corporate and personal infrastructure levels

The establishment and recognition of these boundaries then allows the determination of ownership, maintenance and security responsibilities for the infrastructures concerned. Although in the case of utilising wireless communication technology as a means of supporting telecommunication infrastructure, the physical wireless infrastructure may be located within the property boundary and yet the radio waves used in wireless technology can emanate beyond the physical property boundary.

Wireless Boundaries

The TISN has noted that wireless telecommunication infrastructure is progressively becoming the initial choice and mainstay of many corporate information service infrastructures, this is due to its flexible and functional nature and the perceived lack of physical restraint placed on the physical boundaries of wireless connectivity. However there are some suggested limitations to wireless connectivity and depending on the technology used, wireless technology is categorised as one of the following four types of wireless network and its specified operational distance (TISN, 2004c):

- WWAN (Wireless Wide Area Network) – 10 Km;
- WMAN (Wireless Metropolitan Area Network) – 1 Km;
- WLAN (Wireless Local Area Network) – 100 m;
- WPAN (Wireless Personal Area Network) – 1 m.

Obviously, the detection of stray wireless radio-frequency waves exists beyond their supposed operational distances, the physical confines of buildings and property boundaries and is potentially accessible to those who are external to the business or organisation. Hence the protection and security of the information conveyed across the wireless radio-frequency carrier waves, becomes the responsibility of the owner of the wireless technology

infrastructure (TISN, 2004c). This then raises issues regarding the digital ownership of information, security responsibility and privacy issues within the electronic communications passing across wireless networks and for that matter ultimately the NII.

Digital Boundaries

Electronic communications within the NII can pass across many individually owned communication infrastructures that may exist at any level of the infrastructure model and although the physical boundaries of responsibility between infrastructure levels and sectors is clear, but this is not so identifying digital boundaries. This issue is further complicated when considering the impact of such issues as communication and data security, privacy, and governance.

Clearly, there is a need for further research to establish digital demarcations within critical electronic communication infrastructure to determine the onus of responsibility for data security, privacy, and governance. Unfortunately, the responsibility for securing an electronic information exchange across the publicly accessible NII is not clearly established or defined in the Australian and New Zealand Information Security Management Standard (2001a). It is only advisable that an organisation owning the network or communication infrastructure develops and implements the necessary security policies and practices, and where this expertise is lacking, seek external specialist advice (Standards Australia, 2001a). Although, under the auspice of the Telecommunications Act (1997) the security obligations related to communications is borne by licensed carriers and service providers, who are required to protect the confidentiality of information that relates to the contents of the communication and the affairs or personal particulars of persons related to the communication transmitted.

While neither the Australian and New Zealand information security management Standard (2001a) nor the Telecommunications Act (1997) clearly establishes any point of demarcation between differently owned infrastructures, the general implication is that the protection of any digital communication passing across any communication infrastructure, regardless of ownership, is the responsibility of the infrastructure owner, license carrier or service provider.

Critically, this raises issues of availability that are entrusted to interconnected infrastructures and the influential effect that such dependency or interdependency relationships may have on adjacent infrastructure.

Critical Infrastructure Relationships

As a dependency is a heavily biased or a one-sided relationship and interdependency is a two-way, mutually and equality shared reliance on the availability of multiple critical infrastructure levels, sectors or sub-sectors, which are mutually reliant on one another's availability for continuity of supply and delivery of services.

To illustrate further critical infrastructure interdependency and the complexity of these interactions between various infrastructure sectors, Figure 3 depicts a simplified version of the potential complexity and reliance that sectors have on the availability of services provided by other critical infrastructure systems and sectors, thus illustrating the existence of interdependency relationships (PMSEIC, 2002).

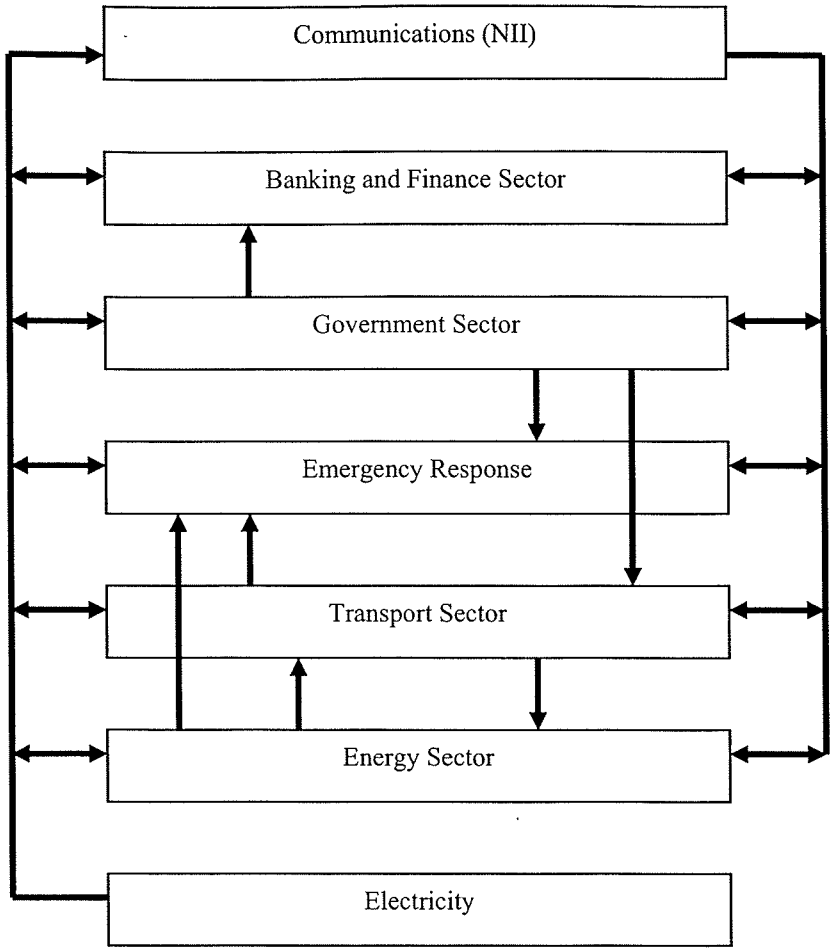

Figure 3: Critical Infrastructure Interdependencies Simplified (PMSEIC, 2002)

The arrows in Figure 3 indicate where the interdependency relationships between infrastructures exist and maps some of the more prominent interdependencies that are apparent within Australia's critical infrastructure (PMSEIC, 2002) and whatever the complexity of the interdependency; they remain a vital consideration to maintaining critical infrastructure service, supply and operation (Marasea & Warren, 2003).

As Figure 3 is an abstraction of high-level interdependencies, the authors propose that the utilisation of system modelling techniques could prove beneficial in illustrating and modelling critical infrastructure dependency and interdependency relationships, at both the high-level infrastructure and the lower-level sub-sectors within the scope of the critical infrastructure model in Figure 1.

Conclusion

The model of Australia's critical infrastructure is largely based upon a number of previously scattered viewpoints that are bought together to represent the basis of the model developed. In its current guise the model recognises the differences that exist within critical infrastructure and attempts to deliver a fair representation of where within the structure, particular levels, sectors and sub-sector that critical infrastructures are situated. This model represents a whole of structure overview and is a starting point for further investigation, refinement and discussion in attempting to categorise critical infrastructures for organisations that own or operate within the setting of Australia's critical infrastructure.

In recognising the relational influence between critical infrastructures, we have attempted to define with greater clarity the terms of dependency and interdependency to bring descriptive certainty to these terms used. In establishing, that influential relationships exist between critical infrastructures we propose that modelling techniques can be utilised to identify and illustrate the existence of influential dependency inter-relationships between critical infrastructures in the Australian context and therefore recognise that further research into comparative relationship modelling and mapping methodologies is required.

The critical infrastructure model (Figure 1) now delivers a scalable representation that clearly establishes and delineates the boundaries between critical infrastructures that will assist organisations in recognising their criticality status, security responsibilities and obligations to critical infrastructure protection, by clearly establishing the physical and digital security obligations of infrastructure owners within Australia's critical infrastructure hierarchy.

References

AGD (2004a) Critical Infrastructure Protection National Strategy, URL:http://www.nationalsecurity.gov.au/ [Accessed: November 21, 2004].

AGD (2004b) Protecting Australia's Critical Infrastructure URL: http://www.ag.gov.au/ [Accessed: May 5, 2005]

AusCERT (2004) *2004 Australian Computer Crime and Security Survey*, AusCERT, Brisbane.

AusCERT (2005) *2005 Australian Computer Crime and Security Survey*, AusCERT, Brisbane.

Australian Government (2004) *Protecting Australia Against Terrorism*, Department of the Prime Minister and Cabinet, Barton.

Booth J. (ed.) (2003) TISN Sector Groups established. *CIP Newsletter,* **1**(2). URL: http://www.tisn.gov.au/agd/www/TISNhome.nsf/Page/Publications [Accessed: November 22, 2004].

Booth J. (ed.) (2004) CIAC adopts National Strategy for CIP. *CIP Newsletter*, **1**(2).URL: http://www.tisn.gov.au/agd/www/TISNhome.nsf/Page/Publications [Accessed: November 22, 2004].

Fleckner A. 2004 Protecting Critical Infrastructure. *Information Age*, October/November: 17-18.

Marasea P. & Warren M.J. (2003) Comparison of Critical Infrastructure Viewpoints. *Proceedings of 4th Australian Information Warfare and Security Conference*, Adelaide.

NCTC (2004) National Counter-Terrorism Committee. Critical Infrastructure Protection in Australia, URL: http://www.tisn.gov.au/agd/www/Cripthome.nsf/Page/CF33E0FF183F9F56CA256CF6007C220E?OpenDocument [Accessed: November 22, 2004].

Pearsall, J., (Ed.) (1998) *The New Oxford Dictionary of English*, Clarendon Press, Oxford.

PMSEIC (2002) Prime Minister's Science, Engineering and Innovation Council. Science and Security, URL: http://www.dest.gov.au/science/pmseic/docments/Science%20and%20Security%20report.pdf [Accessed: November 22, 2004].

Smith, S. (2004) Infrastructure, URL: http://www.parliament.nsw.gov.au/prod/parlment/publications.nsf/0/C6389C30B0383F9ACA256ECF0006F610 [Accessed: November 22, 2004].

Standards Australia (2000) *Wiring Rules AS/NZS 3000.2000*, Standards Australia, Sydney.

Standards Australia (2001) *Installation Requirements for Customer Cabling (Wiring Rules) AS/ACIF S009:2001*, Australian Communications Authority, Milsons Point.

Standards Australia (2001a) *Information Technology - Code of Practice for Information Security Management AS/NZS ISO/IEC 17799:2001*, Standards Association of Australia, Sydney.

Telecommunications Act (1997) *Telecommunications Act 1997. Part 13 - Protection of Communications*. Australia. URL: http://scaleplus.law.gov.au/cgi-bin/download.pl?/scale/data/histact/10/5061/ [Accessed: December 15, 2004]

TISN (2004a) Trusted Information Sharing Network for Critical Infrastructure Protection, URL: http://www.tisn.gov.au [Accessed: November 22, 2004].

TISN (2004b) Key Stakeholders, URL: http://www.tisn.gov.au/agd/www/TISNhome.nsf/Page/Key_Stakeholders [Accessed: November 22, 2004].

TISN (2004c) Wireless Security - Overview for CEO's, URL: http://www.tisn.gov.au/agd/www/TISNhome.nsf/Page/Publications [Accessed: November 22, 2004].

TISN (2004d) Protection of the National Information Infrastructure (NII), URL: http://www.tisn.gov.au/agd/WWW/tisnhome.nsf/Page/National_Information_Infrastructure [Accessed: January 15, 2006].

TISN (2004e) Critical Infrastructure Protection National Strategy, URL: http://www.tisn.gov.au/agd/WWW/tisnhome.nsf/Page/Publications [Accessed: January 15, 2006].

TISN (2004f) About Critical Infrastructure, URL: http://www.tisn.gov.au/ [Accessed: December 16, 2004].

Walker, F. (2004) 'Tisn't working' website comes closer, *The Age*, Melbourne, October 10, 2004, p.3.