11-30-2010

Australian Critical Infrastructure Protection: A case of two tales

Matthew Warren
Deakin University

Graeme Pye
Deakin University

William Hutchinson
Edith Cowan University

DOI: 10.4225/75/57a8366fbefa5
11th Australian Information Warfare and Security Conference, Edith Cowan University, Perth Western Australia,30th November - 2nd December 2010

Australian Critical Infrastructure Protection: A case of two tales

Matthew Warren[1], Graeme Pye[1] and William Hutchinson[2]

[1]Deakin University,
Melbourne, Australia.
matthew.warren@deakin.edu.au

[2]secau - Security Research Centre
School of Computer and Security Science
Edith Cowan University
Perth, Australia.
william.hutchinson@ecu.edu.au

Abstract
The protection of critical infrastructures and the choices made in terms of priorities and cost, all impact upon the planning, precautions and security aspects of protecting these important systems. Often the when choices made is difficult to assess at the time the decision is taken and it is only after an incident that the truth of the choices made become fully evident. The paper focuses on two recent examples of Australian Critical Infrastructure protection and the issues that related to those examples.

Keywords
Australia, Critical Infrastructure Protection, Risk.

INTRODUCTION

The provision and delivery of many of the services that modern society enjoys are the result of ubiquitous critical infrastructure systems that permeate many sectors of the Australian community. Moreover, the integration of technological enhancements and networking interconnections between critical infrastructure systems has heightened system availability and resilience, including the efficient delivery of services to consumers throughout Australia. However, the reliance on these services and their supporting systems is evermore critical: as the removal, temporary loss, degradation or destruction of a single or multiple systems would have a detrimental impact across many sectors of Australian society. With this increasing integration and societal dependence on critical infrastructure systems, their security, availability and protection becomes increasingly significant.

The broader Australian community has an expectation that services such as power and water will be available when desired and that it will be provided as expected in a safe manner. These services and others are provided by various infrastructure systems dedicated to producing and or providing these services seamlessly to all consumers within our modern society. Therefore, by community expectation and necessity, the protection of these critical infrastructure systems is an imperative to governments, infrastructure owners and consumers.
The nature of these critical infrastructure systems and their systematic interconnection display attributes of highly structured, complex interconnected networks that characterise the issues of dependency and interdependency relationships, which by necessity exist between infrastructures to facilitate the supply of services. This is particularly prevalent when considering the energy sector, where for instance the continuity of the supply of electricity is crucial to many other sectors of Australia's critical infrastructure for their ongoing provision of services to the community at large (Scott, 2005).

In the Australian context some common examples of critical infrastructure systems and services to the community, rely on electricity; water; gas and fuel; health services; telecommunications, and banking and financial services to name a few (AGD 2008). Furthermore, other services that are regarded as critical infrastructures in other national contexts may include: air transportation; ground transportation (for example, interstate trucking, railroads, highways, bridges); telephone; cellular telephone; internet; sewers; food distribution and social events (for example, shopping, sports, entertainment) (Smith 2002). However, critical infrastructures are vulnerable and can be damaged, destroyed or disrupted by breakdowns, negligence, natural disasters, accidents, cyber incidents, illegal criminal activity and malicious damage. So it is for these and other reasons that drives the need to protect the continuity of supply against such hazards and threats. It is the aim of government policy and also that of infrastructure owners and operators, to ensure continued supply through identifying and implementing improved security, protective safeguards and analysis in response to the identified threats, vulnerabilities and weaknesses posed (Scott, 2005; Bentley, 2006).

Therefore, protecting critical infrastructure systems from damage and maintaining system functionality, resilience and delivery of the services to the community, requires ethical choices to be made by governments, owners and emergency services, particularly during times of natural disaster.

This paper investigates the choices that arise with regard to managing threats to critical infrastructure systems during times of disaster or when the critical infrastructure system itself becomes the risk.

BACKGROUND

In terms of defining critical infrastructure, the specific Australian determination is as follows (TISN 2004, p.3): "Critical infrastructure 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 on the social or economic well-being of the nation, or affect Australia's ability to conduct national defence and ensure national security."

The diffusion of critical infrastructures permeates across many sectors of the Australian community and economy including banking and finance, transport and distribution, energy, utilities, health, food supply, communications and even key government services and national icons. Some elements are not strictly physical infrastructure and may be 'virtual' in terms of internet-based electronic supply chains for example, or other networks that support the delivery of all important products, information or services (TISN 2003, 2004).Generally, these modern critical infrastructure systems exist securely and seamlessly within our environment and provide many of the services and resources that Australians utilise on an everyday basis; be it at home, work or leisure.

Security and the Environment

Likewise environmental change and its affect can have an impact on human security in a number of ways. If considered from an anthropogenic perspective, it can cause conflict and it can degrade the resources available to human societies (for example, by decreasing biodiversity, by clearing such items as mangrove swamps and forests, by decreasing cropland). Furthermore, such impacts upon the environment can disrupt the very economic base of societies. So to summarise the impact of the natural environment on security, it can be stated that:

- The natural environmental can provide a source of conflict over natural resources and services by their decrease and unequal distribution (Klare, 2001; Renner; 2002);
- Environmental change can affect human security by producing situations that adversely affect human health and well-being for example, drought, food shortages, bio-security threats, chemical contamination and availability of usable land. Also it can directly affect society's infrastructure for example, climate change can cause an increase in bushfires which in themselves can threaten water supplies (by contamination) and power supply (by destruction of power lines and generation facilities);
- Human military and industrial activity can seriously affect environmental health and therefore human security.

However, this is taking a very human-centred approach where the object to be 'secured' is the human and associated systems. A more eco-centric viewpoint would be concerned with the security of regional or global eco-systems. Even the concept of sustainability – both 'weak' and 'strong' which determine whether natural and human capital are considered complements rather than substitutes are considered from a human perspective. In a sense, it is difficult not to do this. However, it is possible to attempt to draw the boundary around a security problem to actively include them on an equal footing with infrastructure systems.

Critical Infrastructure Protection

The implementation of protective measures aimed at securing critical infrastructure systems requires a considered approach, as there are many variables involved in establishing and maintaining a balance between security and functionality of service delivery and system availability. A key part of the greater national infrastructure security picture is the continued availability of critical infrastructure systems that provide and deliver services to the community, to which it has become increasingly reliant.

The underlying premise is that through their pervasiveness nature, these systems and services have become crucial to an improved standard of living for the community generally. Therefore, it is the convenience and availability of these critical infrastructure system services, together with the community's expectations, which leads to potential social issues when the security of these systems is threatened, fails or experiences a reduced level of service and availability. Depending upon the amount of time, how and which critical infrastructure

system or multiple systems thereof are affected, will invariably determine community reaction, incident management and contingency responses that will in turn influence the likely response and recovery actions instigated at governmental, business, personal and wider economic levels.

The perception is that critical infrastructure systems and the services they deliver remain largely in the background, seamlessly providing the services that support the standard of living enjoyed by most highly industrialised societies, with their contribution largely going unnoticed until an incident occurs.

THE 2009 VICTORIAN BUSHFIRE – BACKGROUND

The following case studies highlight the issues that the Victorian Bushfires created in regards to Critical Infrastructure Protection.

The 7th of February, 2009 was a day of unprecedented tragedy in the state of Victoria, Australia. One hundred and seventy-three people died in one of the worst bushfires in Australian history. About 430,000 hectares of land were burnt, as well as 2000 properties and 61 businesses, and the loss of one hundred and seventy-three lives (Teague *et al,* 2009). One of the issues that has not been discussed about the tragic event has been the security implications and in particular the security repercussions in terms of protecting Critical Infrastructure and when the Critical Infrastructure becomes at risk.

CRITICAL INFRASTRUCTURE PROTECTION CASE STUDY 1: WATER

The following Case Study: Victorian bushfires and its environmental security impact, discusses the impact of a natural threat impact a critical infrastructure (Hutchinson & Warren 2009).

Victoria is one of the smaller states in mainland Australia with a population of 5.17 million (Australian Bureau of Statistics, 2008), and its capital city Melbourne has a population of 3.19 million (Australian Bureau of Statistics 2009). This highlights that in the state of Victoria, the majority of the population lives within a single city. This has implications for a number of key services that relate to Melbourne, one of the most important issues being the provision of water.

The majority of Melbourne's water comes from within 160,000 hectares of uninhabited forested catchments north east of Melbourne, Victoria (Melbourne Water 2009a).The impact of the Victorian bushfire was that around 30% of Melbourne's catchments were damaged by fire. This was mostly centred on the O'Shannassy and Maroondah catchments (Melbourne Water2009b). A detailed analysis of the damage is shown in Table 1.

Catchment	**Fire affected**	**Area burnt estimate**	**Share of total reservoir inflow**
Reservoirs with catchment			
Thomson	No	None	36%
Upper Yarra	Yes	About 2% burnt	19%
Maroondah	Yes	About 75% burnt	12%
O'Shannassy	Yes	About 93% burnt	12%
Yan Yean	No	None	2% (not in supply)
Tarago	Yes	About 50% burnt	Nil (not used for Melbourne's water supply)

Table 1: Catchment Impact Table (Melbourne Water 2009b)

During the actual bushfire, a number of key actions were taken and issues raised, regarding water supplies, these included (Roberts 2009):

- The transfer of ten billion litres of water in pipes from the Upper Yarra dam to smaller dams, this was to safeguard the existing water supply;
- The major concern that the run-of ash into reservoirs would contaminate Melbourne's water supplies. If reservoirs were contaminated, it would be contaminated for three months and impact 24% of Melbourne's drinking water.

In reality, the impact of damages caused by bushfire upon catchments areas was not as great as first feared, the actual damage related to (Melbourne Water 2009c) was:

- Damage to water supply infrastructure was limited to minor things such as weir gates;

- The Maroondah aqueduct system escaped major damage but had been experiencing blockages in places by fallen trees and landslides;
- Some movement of soil following the rains since the fires, particularly in the Wallaby Creek area. This is usual with high intensity fires;
- Wallaby Creek sustained considerable damage in burned area and infrastructure;
- A number of buildings have been lost, including the historic Wallaby Creek Quarters complex.

The Victorian bushfires had the potential to damage the water supply of a major global city. Thankfully, the impact was not as severe as first thought. From a critical infrastructure protection perspective, it raises an interesting question about how can the water supplies be protected against such an occurrence. The issue is that reservoirs can only be built in areas of high rainfall; alternative solutions such as building pipelines to transfer water across the state can be very expensive, and they would not be immune to fire damage and could cause an unacceptable environmental impact. Perhaps the announcement of the building of a new desalination plant in the State of Victoria, that will provide 150 billion litres of water a year, could be a the solution from a security perspective (Brumby, 2009).

The summary of issues in relation to this case study was the magnitude of consequences. The extent of the Victorian bushfires was considerable. They created a major risk to Melbourne's water supply which could impact all of Melbourne's population.

Due to the fact the fire spread very quickly, decisions had to be made regarding the protection of people, property and critical infrastructure.

The fire had the potential to impact the majority of the population in the state of Victoria and decisions has to made not just to protect the local population but also larger populations in case the fire spread.

CRITICAL INFRASTRUCTURE PROTECTION CASE STUDY 2: POWER

The second case study is an example of where the critical infrastructure rather than becoming an asset to be protected, it became a major risk and in this case actually caused fires and loss of property and life. The following section is based upon an assessment of the Victorian Royal Bushfire Commission (2010a, 2010b, and 2010c).

The age and maintenance of the Victorian power infrastructure systems became a major during the Royal Commission. During the bushfires on the February 2009, five of the eleven major fires that began that day were caused by failed electricity assets; among the fires was that at Kilmore East, as a result of which 119 people died, this fire was caused by electrical arcing after a conductor (which was probably 43 years old) on the Pentadeen Spur line broke.

Evidence put to the Royal Commission suggests that the age of electricity distribution assets contributed to three fires on 7 February 2009, these were:

- the Kilmore East fire—conductor failure caused by fatigue on a SWER (Single wire earth return) line13;
- the Coleraine fire—fatigue and corrosion leading to a broken tie wire and as a consequence a conductor starting a fire on a SWER line14;
- the Horsham fire—fallen conductor caused by failed pole cap on a SWER line15.

The SWER (Single wire earth return) power infrastructure system is old, having been introduced by the State Electricity Commission of Victoria in the early 1950s to provide a means of electricity distribution to rural areas with low population densities and where small electrical loads need to be widely dispersed. The system could be rolled out relatively cheaply because of its simple design, which consists of a single lightweight, high-tensile conductor mounted on poles. Electricity travels to the customer along the single wire, the current returning through the earth rather than through a second wire.

The SWER design's simplicity offered some bushfire mitigation features because the single line could not clash with other lines and there were fewer poles and less associated infrastructure that could fail. The SWER design limits a SWER line's maximum current, though, and thus the number of customers the line can service; on the SP AusNet network an average SWER line serves just 45 customers. SP AusNet recognises that the SWER

network is reaching thermal capacity and that some SWER lines are already overloaded. This raises questions about the SWER system's capacity to meet present and future demand and maintain supply quality.

Against the background of aging Victorian power infrastructure, the Royal Commission, identified a number of key issues with the systems, which are:

- Aging conductors – a key report of SP AusNet's conductor study noted that the great majority of conductor failures on the organisation's network involved high-voltage conductors and that this represented a 'considerable risk to the business from a public safety and bushfire perspective'. The report said, 'In the absence of planned conductor replacement programs, failure rates may begin to increase at an exponential rate due to the increasing proportion of [the] conductor fleet approaching current failure age ranges';

- Insulator failure - Insulator failure can result in pole fires, cross-arm fires, conductor drops, conductor clashing, and conductor contact with the ground. Such incidents constitute bushfire risks;

- Aging assets - There is a substantial peak in the age of assets, indicated by the example of wood poles. In 2004 there are 37,000 wood poles 50 years and older, however this will increase to approximately 62,000 by 2010 based on average replacement of 1,500 wood poles per year;

- Impact of external elements - studies examined the circumstances of the tie-wire failure that led to the Coleraine fire on 7 February. The study found that the typical life span for zinc galvanising on tie wires of that kind is about 40 years and that the Coleraine tie wire was probably more than 40 years old. The study noted the galvanising on that tie wire had been consumed by external elements, greatly increasing the corrosion rate and leading to pitting and the initiation of fatigue cracks on the tie wire.

The key recommendations from the Royal Commission in relation to power infrastructure were:

- The progressive replacement of all SWER (single-wire earth return) power lines in Victoria with aerial bundled cable, underground cabling or other technology that delivers greatly reduced bushfire risk. The replacement program should be completed in the areas of highest bushfire risk within 10 years and should continue in areas of lower bushfire risk as the lines reach the end of their engineering lives

- The progressive replacement of all 22-kilovolt distribution feeders with aerial bundled cable, underground cabling or other technology that delivers greatly reduced bushfire risk as the feeders reach the end of their engineering lives. Priority should be given to distribution feeders in the areas of highest bushfire risk.

The Victorian state government premier response to the power-line replacement recommendations was "it literally out of this world, it's $20b plus, and secondly, you could do all of that and you still get fires that are caused by machinery… lightning… arson." The Victorian state Government will set up a $2m taskforce, to work with industry to identify high priority areas for upgrading powerlines (ABC, 2010).

The summary of issues in relation to this case study again was the magnitude of consequences. The magnitude of the Victorian bushfires was considerable. A major difference in this case study was that in many cases the critical infrastructure caused the fires and by doing so destroyed parts of itself. The initial impact of the failure was localised in the vicinity of the fire, but due to environmental conditions these fires quickly spread. There was not a major risk to Melbourne's power supply immediately, even though a later fire in Gippsland did put Melbourne's power supply at risk by threatening the power cables from the La Trobe power station complex.
Due to the fact the fire spread very quickly, decisions had to be made regarding the protection of people, property and critical infrastructure. At the time there was no realisation that the power infrastructure had caused the fires.

The loss of the power service impacted localised communities and in many cases impacted their ability to fight the fires or communicate the situation or developing situation.

CONCLUSION

Security implications are inherent in all critical infrastructure related protection decisions. Decision makers should be aware of the stance and assumptions they are making in regard to these issues and be aware of the implications of the stand point taken. The issue is that protection of critical infrastructure can easily be

identified, but when the critical infrastructure becomes the risk, especially with ageing critical infrastructure, this could pose new critical infrastructure protection issues.

REFERENCES

ABC (Australian Broadcasting Corporation) (2010) John Brumby details the State Government response to the Bushfires Royal Commission, URL: http://www.abc.net.au/local/stories/2010/08/27/2995659.htm Accessed 1st September, 2010.

Australian Bureau of Statistics (2008) *Report 1301 - Year Book Australia*, 2008, Canberra, Australia.

Australian Bureau of Statistics (2009) *Report 3218 - Regional Population Growth*, Australia, 2007-08, Canberra, Australia.

AGD (2008) Critical Infrastructure Protection, Australian Government Attorney-General's Department.URL: http://www.ag.gov.au/www/agd/agd.nsf/Page/Nationalsecurity_CriticalInfrastructureProtection Accessed: April 2008.

Bentley A. (2006) *Infrastructure: Critical Mass*, CSIRO Solve, No.7.

Brumby, J. (2009) *Australia's biggest desalination plant to secure water and jobs*, Victorian State Government, 30th July.

Hutchinson, W., Warren, M. (2009) Security as an element in environmental assessment and decision making, *Proceedings of The 2009 Conference of the Australia and New Zealand Society for Ecological Economics (ANZSEE)*: Green Mileage in the Global Meltdown: An Ecological Economics Way Forward, Darwin, Australia, 27th-30th October 2009.

Klare, M.T. (2001) *Resources Wars: The New Landscape of Global Conflict*, Metropolitan Books, New York.

Melbourne Water (2009a) Bushfires in Catchments, URL: http://www.melbournewater.com.au/content/water_storages/bushfires_in_catchments/bushfires_in_catchments.asp Accessed, 21st September, 2009.

Melbourne Water (2009b) Catchment Impact Table, URL: http://www.melbournewater.com.au/content/water_storages/bushfires_in_catchments/february_2009_-_catchment_impact_table.asp Accessed, 21st September, 2009.

Melbourne Water (2009c) *Bushfire Recovery Community Update*, 19th May.

Scott G. (2005) *Protecting the Nation*, AUSGEO News (Geoscience Australia), Issue No.79.

Smith R. (2002) *Complexities of Simulating Domestic Infrastructure Protection*, Titan Systems Corporation, Orlando, FA, USA.

Teague, B., McLeaod, R., Pascoe, S. (2009) *2009 - Victorian Bushfire Royal Commission Interim Report*, Victorian State Government, Melbourne.

TISN (2003) *Fact Sheet: What is Critical Infrastructure?* Trusted Information Sharing Network (TISN), Canberra.

TISN (2004) Critical Infrastructure Protection National Strategy, Trusted Information Sharing Network (TISN).URL: http://www.tisn.gov.au/agd/WWW/rwpattach.nsf/VAP/(930C12A9101F61D43493D44C70E84EAA)~National+CIP+Strategy+2.1+final.PDF/$file/National+CIP+Strategy+2.1+final.PDF Accessed: April 2008.

Renner, M. (2002) The Anatomy of Resource Wars, *World Watch Paper 162*, Worldwatch Institute, USA.

Victorian Royal Bushfire Commission (2010a) *Final Report Volume 1- The Fires and the Fire-related Deaths,* Victorian Parliament, Australia, ISBN 978-0-9807408-2-0.

Victorian Royal Bushfire Commission (2010b) *Final Report Volume 2 - Fire Preparation, Response and Recovery*, Victorian Parliament, Australia, ISBN 978-0-9807408-3-7.

Victorian Royal Bushfire Commission (2010c) *Final Report Summary, Victorian Parliament*, Australia, ISBN 978-0-9807408-1-3.