Critical infrastructure protection: an ethical choice

Citation:

DOI: [10.4018/978-1-60960-573-5.ch011](http://dx.doi.org/10.4018/978-1-60960-573-5.ch011)

©2011, IGI Global

Reproduced with permission.

Downloaded from DRO:
[http://hdl.handle.net/10536/DRO/DU:30036184](http://hdl.handle.net/10536/DRO/DU:30036184)
Chapter 11
Critical Infrastructure Protection: An Ethical Choice

Graeme Pye
Deakin University, Australia

Matthew Warren
Deakin University, Australia

William Hutchinson
Edith Cowan University, Australia

ABSTRACT
The protection of Australian 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 choices made will have an ethical imperative that 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. This is the focus of this discussion that highlights the issues of earlier resource funding choices made and how an ethical choice had to be made, with regard to protecting the security of a water supply infrastructure, or that of a community under the threat of bushfire as outlined in the case study.

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 ever more 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 system 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.

Australia’s modern industrialised society, like those of other western nations, is increasingly reliant on the crucial services delivered by various physical and virtual infrastructure systems to maintain the comfortable standard of living and convenience that the population largely enjoy. Furthermore, the diffusion of information and communication technologies and their incorporation into these crucial systems enables greater system interconnections, which form relationally cooperative networks that facilitate communication, automation and control of infrastructure services supply. Thereby, the maintenance of high-levels of system availability, responsiveness and resilience in terms of their ongoing service supply is required, as is largely the expectation of the community and individual 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; telecommunication; 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 (interstate trucking, railroads, highways, bridges); telephone; cellular telephone; internet; sewers; food distribution and social events (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 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).

The impact of disrupting one or more of these services that critical infrastructures supply and the potential inconvenience to the wider community is an ongoing concern to national decision makers. This is due largely in part to the physical magnitude of many of these infrastructures and the complexity of their interconnections and relationships with other systems. Furthermore, system availability coupled with system security analysis of the infrastructure operation and environment may provide sufficient insights into the potential vulnerabilities of these assets. Although this represents a significant challenge, critical infrastructure industry owners and operators including the various levels of government must remain cognisant of the potential consequences
of system compromise. This requires critical infrastructure stakeholders to seek ways in which to address, analyse, cope, plan and comprehend the complexities of the twenty first century security of critical infrastructures (Smith, 2002).

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 research investigates the ethical choices that arise with regard to managing threats to critical infrastructure systems during times of disaster, which may impinge upon the availability and quality of the resources that critical infrastructure systems supply to the community.

At the outset, a background discussion will provide an understanding of what critical infrastructures are in the Australian context and describe some past events that exemplify the criticality of these systems to the community. The issue of critical infrastructure system protection is broadly explained, before outlining the ethical issues surrounding the critical infrastructure systems case study presented. Finally, a discussion of the ethical choices made in response to the evolving situation within the context of the case study is undertaken and outcomes are discussed, before presenting conclusions and identifying future research opportunities.

**BACKGROUND**

In terms of defining critical infrastructure, the specific Australian determination is as follows (TISN 2004b, 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, 2004b). 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.

**Ethical Decision Making**

In society, whether in a business context or in a day to day situation, the majority of decisions that are made are based upon an ethical viewpoint. The ethical reasoning could be due to a number of factors including political views, upbringing and personal values have long been associated with individual decision behaviour. There has been extensive research into the ethical decision making in a business context (Hunt & Vitell (1986), Singhapakdi and Vitell (1991); Mayo and Marks (1990), Hunt and Vasquez-Parraga (1993), Herndon (1996) and Harrington (1997)).

The role played by personal values in decision making within an organization is less clear (Fritze 1995). Prior research into individuals ethical decision making (Wagner & Sanders 2001) had determined that individual characteristics, such as religion and the issue under consideration are expected to affect the ethical evaluation that an individual goes through based on their underlying ethical philosophies and cognition (level of moral development). The evaluation stage of ethical decision making involves an individual evaluating or
determining the rightness or wrongness of aspects of a particular issue. The individual considers aspects or alternatives of the issue such as whether he deems them to be just or unjust, acceptable to himself or to others, conforming to society and government expectations. Ethical evaluations result in a judgment regarding the ethical issue and also impact the intended actions of the individual. An ethical judgment is the determination of an action as being ethical or not ethical. An individual’s intention is the probability that they will engage in an action presented to them as an outcome to an ethical situation.

Wagner and Sanders (2001) proposed a theoretical model (as shown by Figure 1) which illustrated the stages that an individual passes through in determining a course of action when confronted with an ethical issue. An individual is considered to be an active agent within the context of their social, economic and organizational environments.

In a security context, ethical decision making may not always apply. In a security or emergency situation, the magnitude of consequences is the main issue that has to be considered. Jones (1991) identified six major factors that should be considered when the magnitude of consequences are reviewed. The major factors are:

**Magnitude of Consequences**

The magnitude of consequences of the moral issue is defined as the sum of the harms (or benefits) done to victims (or beneficiaries) of the moral act in question. For example, an act that causes 1,000 people to suffer a particular injury is of greater magnitude of consequence than an act that causes 10 people to suffer the same injury.

**Social Consensus**

The social consensus of the moral issue is defined as the degree of social agreement that a proposed act is evil (or good). For example, the evil involved in discriminating against minority job candidates has greater social consensus than the evil involved in refusing to act affirmatively on behalf of minority job candidates.

**Probability of Effect**

The probability of effect of the moral act in question is a joint function of the probability that the act in question will actually take place and the act in question will actually cause the harm (benefit) predicted. For example, producing a vehicle that would be dangerous to occupants during routine driving has greater probability of harm than producing a vehicle that endangers occupants only during rear-end collisions.

---

*Figure 1. Decision making in an ethical context*
Temporal Immediacy

The temporal immediacy of the moral issue is the length of time between the present and the onset of consequences of the moral act in question (shorter length of time implies greater immediacy). For example, releasing a drug that will cause 1 percent of the people who take it to have acute nervous reactions soon after they take it has greater temporal immediacy than releasing a drug that will cause 1 percent of those who take it to develop nervous disorders after 20 years.

Proximity

The proximity of the moral issue is the feeling of nearness (social, cultural, psychological, or physical) that the moral agent has for victims (beneficiaries) of the evil (beneficial) act in question. For example, layoffs in a person's work unit have greater moral proximity (physical and psychological) than do layoffs in a remote plant.

Concentration of Effect

The concentration of effect of the moral act is an inverse function of the number of people affected by an act of given magnitude. For example, a change in a warranty policy denying coverage to 10 people with claims of $10,000 has a more concentrated effect than a change denying coverage to 10,000 people with claims of $10.00.

Security and the Environment

Likewise environmental change and its effect 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:

- Future changes could provide a source of conflict over natural resources and services by their decrease/depletion and unequal distribution (Klare, 2001, Renner, 2002), e.g. conflict over water, failure of water supplies for major cities;

- 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.
Modern Critical Infrastructure Systems

Modern infrastructure systems are the product of a steady development, improvement and expansion throughout the twentieth century into the present day. Furthermore, the incorporation of new technologies continues to improve the functionality and reliability of these systems and the essential services they deliver to the greater community. Modern infrastructures deliver a variety of services to the modern industrialised societies that have permeated into both the public and private lives of its citizens. This pervasive phenomenon has increasingly become the focus of concern from a national security perspective, particularly with regard to protecting critical infrastructure systems and maintaining system availability.

The conceptual notion of a national critical infrastructure was ushered into the public arena in the mid 1990s when the United States began to acknowledge that a set of infrastructure facilities and services were critical to the ongoing well-being of the nation and its citizens. Initially the US critical infrastructure systems and organisations identified were those providing electricity, water, fuel supply, communications, transport, the finance sector, government and public services. Although infrastructure system failures do happen and multiple failures are possible, the belief was that as long as they were not significant or long term in duration, there would be no threat to the governance of the nation or the well-being of the population. It remains evident that infrastructure facilities and services are critical to government and the people and require protection at times of civil unrest, and wars where it is essential to protect food, water and energy supplies (Jones, 2007a).

Furthermore, during the twentieth century the advances in technology and its incorporation, particularly the internet, has led to the realisation that physical protection is simply not enough. This connectivity introduces another avenue to perpetrate an act involving an infrastructure system without being physically present to commit the act. Many of these changes in the security attitude and protection of critical infrastructures are the result of various incidents that have occurred since the 9/11 attacks of 2001 in the US. This has resulted in the adoption of tighter security attitudes being adopted by other nations (Jones, 2007a).

Additionally, it is the benefits of the technological capabilities incorporated into today's infrastructure systems that are a measure of a nation's economic prosperity and development. The outcome is high quality and reliable infrastructure services that contribute to higher living standards for the community generally. Additionally, these infrastructure systems play an important part in attracting private sector investment that in turn contribute to ongoing national economic growth and increasing prosperity (COAG, 2007).

Modern infrastructures are prevalent across numerous sectors of today's community such as energy, utilities, transport, communications, health, food supply, finance, manufacturing, mining, government services and national icons (NCTC, 2004). Although not a fully inclusive list, it is through these underpinning infrastructure distribution networks that essential products and services reach the community and other jurisdictions as required. For the most part, the infrastructures identified here are relevant to most industrialised nations, with a few variations to those listed attributing to specific needs or a particular approach taken by a particular nation towards infrastructures that underpin the standard of living (Marasea & Warren, 2004).

Furthermore, it is the convenience and availability of the infrastructure services, together with community expectations, that potentially leads to adverse social issues when these systems fail, falter or experience a reduced level of service supply or availability to the community. Depending upon magnitude and which infrastructures or multiple infrastructures are affected, will invariably determine the community reaction and influence the likely response contingencies evoked at govern-
mental, business, personal and wider economical levels (Pye & Warren, 2008; 2009).

**Exemplifying the Criticality of Infrastructures**

Modern industrialised societies are increasingly reliant on key infrastructures and their support systems to reliably produce and deliver their services. Electricity supply and distribution, water supply, fuel supplies and distribution, telecommunication services, transportation and distribution systems and emergency response services to list some of these infrastructures systems, are critical to a modern industrial society. Furthermore, consider adding to these the stock exchange, banking and financial systems, health services and food supply systems. It soon becomes apparent that the potential impact upon the community is significant if such critical infrastructure systems were to fail (Slay & Koronios, 2006).

The loss of these systems even for a short time can result in significant, severe disruptions to the activities of business and the greater community at large, as evidenced by the Victorian gas crisis in 1999. In this instance, the state of Victoria, Australia was without gas supplies for a number of weeks with the associated costs to business and government estimated in the billions of dollars; not discounting the major inconvenience presented to householders with no gas for cooking and heating purposes (ANAQ, 2000).

Two other relevant examples of critical infrastructure system failure were the separate 1998 power outages following generator and grid infrastructure failures in Brisbane, Australia and Auckland, New Zealand. In both cases, sections of the cities were without reliable power supplies and government and business alike had to operate in this environment for an extended period (ANAQ, 2000). The recent gas plant explosion at the Apache Energy’s facility on Varanus Island off Karratha in the Pilbara region of Western Australia (WA) on 3rd of June 2008 exemplifies another critical infrastructure system failure. The explosion and fire affected gas export pipelines that carry the gas supply south to the domestic market and cut supply by one-third indefinitely, with estimates of at least two months before even partial gas production could resume (Williams, 2008; Le May, 2008). As Apache Energy was the second biggest supplier of gas, the WA state government had no option but to ration gas supplies to the industrial, manufacturing and mining sectors forcing sharp cutbacks in production for at least two months due to their dependency on a consistent supply of gas (Chambers, 2008; Gosch, 2008).

Furthermore, from an information and communications technology (ICT) perspective, a recent Australian federal government review of its use of ICT found that power agencies had raised concerns regarding the electricity supply to federal government data centres in the Australian Capital Territory (ACT). The critical issue was that the ACT’s single electricity distribution grid is currently fed by two supply feeds from the larger New South Wales (NSW) electricity supply grid, with one feed supplying 85 percent of the ACT’s electricity requirements and the smaller 15 percent feed only supplying the immediate localised suburban area of Fyshwick. What this electricity supply reliance imbalance indicates, was that the smaller electricity power feed was insufficient to support government agency needs and that government agency data centres situated in Canberra remain vulnerable, due to their ongoing dependence on the larger, single ACT electricity supply feed (Gershon, 2008).

Additionally, during the summers of 2007, 2008 and 2009 Victoria’s electricity generation, distribution and transmission system has been unable to cope with demand due to a combination of extreme hot weather and bushfire events (Dowling, 2009). During the 2009 heatwave, electricity demand outstripped supply capability resulting in rolling ‘blackouts’ across the state affecting more than one hundred thousand homes, businesses and industries (Dobbin & Dowling, 2009;
Moran, 2009). This illustrates the consequences of a dependency relationship, as exhibited by the electrified suburban train system. The contracted service provider was forced to cancel nearly 40 percent of its services on the worst day leaving many passengers stranded, because of intermittent power supplies and issues regarding the buckling railway tracks' inability to cope with the extreme heat, even when power was available (Economou, 2009; Houston & Reilly, 2009; Lucas, 2009a; Lucas, 2009b).

In essence, what these examples illustrate is the importance and criticality of maintaining service supply security of critical infrastructure systems. This is a consequence of the pervasiveness of the services these systems provide and the sophistication of information technology (IT) functioning within these systems, coupled with physical service supply and community expectations. This reliance upon critical infrastructure systems has permeated into nearly every corner of Australian daily life, with the community now largely dependent upon the many infrastructure systems and services they deliver for their day-to-day activities, which the community largely takes for granted, and feel secure in the expectation that critical infrastructure system services remain available when needed and on demand.

It is at this point, when the greater community cannot do without the services these systems provide, that they become critical infrastructures because of the crucial services they deliver to the ongoing wealth and well-being of society in general. Therefore, the logical extension of this assumption is that service assurance and integrity of the system progressively attains a condition that is fundamentally essential to most modern, secure, industrialised and stable societies. Additionally, it is from the national security perspective that governments begin to realise the potential threat of interrupting, denigrating performance or the destruction of a nation's critical infrastructure systems and the potential flow-on effects of such scenarios. Therefore, in order to effectively plan for and protect critical infrastructure systems, it is imperative that a comprehensive understanding of the system structure, operational intricacies, security characteristics and vulnerabilities is attained, which is central to developing a considered assessment of the soundness of these physically large and geographically distributed systems (TISN, 2006).

As identified, critical infrastructure systems provide essential services and capabilities to modern industrialised societies that have become an intrinsic concern in terms of national security and the potential security vulnerabilities of their technological interconnection, networking and increasingly the reliance on the availability of services that critical infrastructure systems deliver to the community. Therefore, the protection of critical infrastructure systems continues to be the subject of security scrutiny as national governments recognise the importance of maintaining secure system availability as an imperative to the national interest.

**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 that, largely, have 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

221
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.

Protecting Critical Infrastructures: Why?

The primary area that continues to emerge as the central theme to critical infrastructures is security and the protection of critical infrastructure systems from damage, attack or disaster. This requires continued vigilance and a focus on sustaining and ameliorating the resilience of critical infrastructure systems and their ability to maintain service integrity, recover and remain available in the face of adverse conditions and events.

Modern societies and governments continue to invest in infrastructure systems to meet current demand and future needs and furthermore, these infrastructure systems have continued to evolve through the integration of new technologies. This has changed infrastructure systems from simple, localised, single focus systems to more distributed, complex and integrated ones to increase efficiency of operation, improve service availability and reliability and offer greater consumer choice and safety generally. The alternative of diminishing infrastructure systems moves the society it supports toward less comfort and safety, from plenty to scarcity, from richness to want. Societies and governments recognise their essential dependence on these systems and adopt policies and processes to distribute infrastructure and services widely and to protect them from physical damage and misuse (Lukasik et al., 1998).

The physical security threats to critical infrastructure system assets are many and varied and can manifest themselves as fires, floods, natural disasters, accidents, sabotage, human error, lightning strikes, earthquakes and climate change, to name some of the more recognisable physical threat possibilities. The likelihood and frequency of such physical events occurring depends on location and geographical environmental characteristics.

However, critical infrastructure systems remain exposed to a myriad of operational and environmental threats, each with a unique ability to disrupt operations. For example, road networks are vulnerable to flooding, landslides, traffic congestion and major accidents. Telecommunication networks are vulnerable to denial of service attacks, computer viruses, targeted infrastructure attacks and congestion. In fact, all critical network infrastructures, to some degree, are vulnerable to either technological or natural hazards and it for these and other reasons that protection of critical infrastructure systems remains an important necessity (Murray & Grubesic, 2007) One such example in the Australian context is the threat of bushfires to the availability of critical infrastructures services in the form of Melbourne’s metropolitan water supply.

Protecting Water Infrastructure and Catchments

As an example of the need to protect critical infrastructures, maintaining a safe, secure and reliable water supply to any population centre, especially a large city such as Melbourne, is an imperative across all levels of government. In this instance approximately 80 percent of Melbourne’s drinking water is collected and stored in catchments
located in the Yarra Ranges east of Melbourne (Melbourne Water, 2009a).

The catchment areas consist of some 157,000 hectares of protected native forests that naturally filter the rainwater as it flows into the catchment reservoirs via creeks and rivers. These areas have been closed to the public for over 100 years to protect the quality of the water and to protect against unauthorised public entry, erosion and bushfires. These actions reduce the risks of disease or contamination of the drinking water supply system and the likelihood of bushfires occurring within the catchment bushland areas (Melbourne Water, 2009a).

The bushfire threat is of particular concern to the quality and security of the drinking water supply. It is the resultant loss of vegetation that negates the natural filtering effect and fails to slow the flow of water, thereby enabling contaminated water to flow into the reservoir. Another long term effect is that the loss of mature forest trees results in forest regeneration activity where the immature saplings can use up to 50 percent more water than mature trees (Melbourne Water, 2009a).

The following case study outlines just such a scenario as part of the ethical discussion undertaken here with regard to protecting critical infrastructure systems.

THE CRITICAL INFRASTRUCTURE PROTECTION CASE STUDY

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).

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 (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 environmental security repercussions.

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 percent of Melbourne’s catchments were damaged by fire. This was mostly centred on the O’Shannassy and Maroondah catchments (Melbourne Water, 2009b). A detailed analysis of the damage is shown in Table 1.

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;
- Identifying the major concern that the ash residue left from the bushfire would be transported by subsequent rain water ‘run-off’ into reservoirs and would contaminate Melbourne’s water supplies. If reservoirs were contaminated, it would be contaminated for three months and impact 24 percent of Melbourne’s drinking water.

Fortunately, the impact of damages caused by bushfire upon catchments areas was not as great as first feared and was limited as follows to (Melbourne Water, 2009c):
Table 1. Catchment impact table (Melbourne Water, 2009b)

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

- 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 you can protect against such an occurrence. The issue is that you can only build reservoirs 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).

Ethical Analysis of Case Study

As discussed previously, when looking at a security or emergency related situation, it is the magnitude of consequences that have to be assessed when making decisions. As an example, the Victorian bushfires and its environmental security impact will be studied using the Jones (1991) consequence model. The major factors are:

Magnitude of Consequences

The magnitude of the Victorian bushfires was considerable. The outcome of the fire was 430,000 hectares of land were burnt, as well as 2000 properties and 61 businesses. Melbourne’s water supply was at risk and one hundred and seventy-three people died.

Social Consensus

The social consensus was that the fire had to be stopped at all costs.

Probability of Effect

The impact of the effect of the fire was that it was far greater than anything experienced before.
Temporal Immediacy

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

Proximity

The fire had the potential to spread directly into Melbourne, a city of over three million people.

Concentration of Effect

The fire had the potential to impact the majority of the population in the state of Victoria.

Post Script

The Australia’s Commonwealth Scientific and Industrial Research Organisation (CSIRO) undertake a major review on the impact of climate change and infrastructure on behalf of the Victorian State Government.

The CSIRO Report (CSIRO, 2006) predicts that enhanced conditions for major bushfires events in the catchments of dams and reservoirs will generate immediate impacts on water quality and availability as well as medium-term reduction in water yield. Costly short-term water quality solutions will be needed should this occur in major catchments.

The main areas of concern are with regard to the Bushfire and Water (CSIRO, 2006):

- An increase in bushfire within the main water catchment for cities and towns causing an immediate loss of water supply from ash, debris, sediments and fire fighting chemicals affecting the water quality of the dams and reservoirs. The Canberra Fires in 2004 are an example of this impact;
- A financial cost impact resulting from a bushfire through key water harvesting catchments could also be the technology expenditure to utilise the water affected in the short term through, for example installation of cleaning or membrane filtration technology to treat water to meet quality standards. Such technology is not currently installed for any of the major Melbourne catchments;
- Financial impact to water dependent industries and water supply agencies;
- Significant community hardship and outrage;
- Expensive transport of water and extraction from other water constrained areas;
- Several years of reduced water yield from catchments due to increased water use during tree regrowth.

The CSIRO Report rates the chance of catastrophic bushfire in the state of the Victoria as being (CSIRO, 2006):

- **2050**: Prediction of a Moderate–High risk level of a catastrophic bushfire occurring in Victoria;
- **2070**: Prediction of a High–Extreme risk level of a catastrophic bushfire occurring in Victoria;

It may be postulated that the catastrophic bushfire event of 2009 may have occurred forty years to early in terms of the CSIRO Report, however this event may serve to exemplify and draw attention to the potential impact of future bushfires in Victoria.

OUTLINING THE ETHICAL DILEMMA

The ethical dilemma is the allocation of bushfire fighting resources in relation to the protection of the water supply infrastructure catchment areas and managing the water supply under threat.
Critical Infrastructure Protection and the Victorian Bushfires

The infrastructure is the contamination of the public water supply through the damage caused to parts of the water supply storage and catchment areas including the water grid infrastructure.

The Ethical Perspectives

The Ethical issues relate to a number of different situations:

- **Consumers:** should the people of Melbourne expect that their water supply should be secured?
- **Melbourne Water:** is the role of Melbourne Water just to provide water to its customers or to provide a secure service that is available under any situation?
- **Fire Fighters:** should fire fighting resources be moved from protecting centres of population (protecting people and homes) to critical infrastructure protection (protecting the water supply of Melbourne)?

As well as the ethical issues, there are also a number of environmental issues that cause an impact upon this decision making:

- The impact of a lack of resources due to state governmental budget cuts for the funding for full time and casual fire fighters (financial issue);
- The impact of a lack of planned burning to reduce fuel loads and the impact this would have upon localised eco-systems (ecological/social issue);
- Possible link to global weather change (global issue).

All these ethical issues and perspectives each individually raise relevant issues for priority resource management, protection including aspects of government budgetary consideration and financial investment in infrastructure security. In reality choices are made in an attempt to strike a balance between perceived risk to consumers, protecting and securing the resource and the likelihood of an adverse water infrastructure incident impinging upon consumer well-being, including the cost.

**SOLUTIONS AND RECOMMENDATIONS**

As this ethical dilemma highlights, the choices are never clear cut or straightforward, but with the benefit of hindsight and a lessons learned approach, this can aid in evaluating, planning and targeting strategic investment in the future. It must be acknowledged that those making decisions at the time of any incident do so with the best intentions acting on the information at hand. In this situation the choice was to concentrate on the protection of critical water infrastructures and the threat to public health through contamination of the water supply or to the fighting fight the bushfires threatening individual people and their homes.

**FUTURE RESEARCH DIRECTIONS**

The Critical Infrastructure Protection Case study helps to identify and analyse the impact that critical infrastructures protection and weather change can have upon a society. The aim is of the future research is to develop security models that will help to protected against the future security issues that related to critical infrastructure protection and in particular the impact that weather changes could have upon those key critical infrastructures.

**CONCLUSION**

Security implications are inherent in all but the very minor environmentally related decisions
made. Decision makers should be aware of the stance and assumptions they are making with regard to these issues and be aware of the implications of the stand point taken. Those who wish to promote sustainable use of natural resources should also embrace the notion of security as it is a pragmatic way to encourage politicians and the public to consider other options rather than the biased traditional economic and political approaches taken to come to a decision. The problem of water security in Australia will become an even greater issue and the ethical considerations will also become a greater problem.

REFERENCES


**ADDITIONAL READING**


**KEY TERMS AND DEFINITIONS**

**Critical Infrastructure:** The 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.

**Risk:** The possibility of suffering harm or loss; danger.

**Security:** Something that gives or assures safety, as: (1) Measures adopted by a government to prevent espionage, sabotage, or attack; (2) Measures adopted, as by a business or homeowner, to prevent a crime.

**Threat:** An indication of impending danger or harm.