



ARCHIVED - Archiving Content

Archived Content

Information identified as archived is provided for reference, research or recordkeeping purposes. It is not subject to the Government of Canada Web Standards and has not been altered or updated since it was archived. Please contact us to request a format other than those available.

ARCHIVÉE - Contenu archivé

Contenu archivé

L'information dont il est indiqué qu'elle est archivée est fournie à des fins de référence, de recherche ou de tenue de documents. Elle n'est pas assujettie aux normes Web du gouvernement du Canada et elle n'a pas été modifiée ou mise à jour depuis son archivage. Pour obtenir cette information dans un autre format, veuillez communiquer avec nous.

This document is archival in nature and is intended for those who wish to consult archival documents made available from the collection of Public Safety Canada.

Some of these documents are available in only one official language. Translation, to be provided by Public Safety Canada, is available upon request.

Le présent document a une valeur archivistique et fait partie des documents d'archives rendus disponibles par Sécurité publique Canada à ceux qui souhaitent consulter ces documents issus de sa collection.

Certains de ces documents ne sont disponibles que dans une langue officielle. Sécurité publique Canada fournira une traduction sur demande.

Power, water, health, communication systems, banking and transportation are among the essential services and systems that underpin a nation's security, community development and economic progress. At all levels of Australian government (federal, state and territory, and local) protection of these critical infrastructure assets, the majority of which are now owned and operated by the private sector, has been a major focus of national security strategy.

This Briefing Paper traces the policy focus on critical infrastructure protection in Australia over the last 30 years. The author notes that two major terrorist events – the 1978 Hilton Hotel bombing in Sydney, and the 9/11 attacks on the USA – were key drivers in policy change. This paper reviews how such policy responses were influenced by the shift in ownership of assets from the public to private sector, and policy transfer from the UK and USA. The paper concludes by identifying potential areas for research, including the state's role as both regulator and owner-operator of some critical infrastructure assets.

Ms Kate O'Donnell is a Senior Officer with the Department of Transport and Main Roads, seconded to CEPS in 2011 as an Industry Practitioner. Ms O'Donnell has provided expert advice to the Government Coordination and Vulnerable Infrastructures Project, as the Project was mapped and scoped during 2011. This Briefing Paper is a synopsis of Ms O'Donnell's Masters (Honours) in Criminology and Criminal Justice thesis, undertaken while seconded to CEPS.



Dr Ruth Delaforce
Editor
CEPS Research Fellow

The development of Australia's federal critical infrastructure policy, 1978 – 2010

Ms Kate O'Donnell

Overview

Australia's strategy for managing national security is set out in a number of complex and interrelated policy documents that span multiple agencies. The strategy for protecting what is now known as "critical infrastructure" and "designated critical infrastructure" is only one part of this complex policy fabric that has developed over time. This paper summarises key parts of the federal critical infrastructure (CI) protection policy trajectory in the period 1978 – 2010.

Research Questions

The research was designed to answer the following questions:

1. How has Australia's federal critical infrastructure policy developed in the 30 year period from 1978 to 2010, and why?
2. How and to what extent has that development reflected:
 - a. A direct influence of policy transfer from the United Kingdom (UK) and the United States of America (USA) to Emergency Management in Australia?
 - b. Industry's changing role over the 30 year period?
 - c. Contributions to the current federal legislative framework for critical infrastructure protection?

Research Methodology

The research methodology drew on historical-comparative research theory and an analytical framework of policy transfer. The data collection methodology involved three phases. First, material was gathered in the form of primary source documents such as government policies, government documents, independent reviews, annual reports, official reports, speeches, legislation, Hansard, parliamentary debates, official newsletters, media releases and published works to identify relevant policy documents and generate draft definition and policy chronologies.

Second, analysis of available data and literature elucidated general themes of the period, including a policy trajectory marked by security incidents, reviews, changing concepts and definitions of critical infrastructure, policy transfer, and a fundamental shift in ownership of critical infrastructure from predominantly state-owned, to predominantly private sector owned and operated. These initial themes were used to identify the areas where supplementation through interviews would be valuable and themes could be tested.

Finally, seven semi-structured interviews were conducted with current and former

senior policy-makers. Elite senior executives with first-hand experience in the field and were identified through the non-probability snowball sampling technique. Formal interviews were supplemented by personal communications with some interviewees prior to, and following, the interviews. The interviews and personal communications were both corroborative in terms of the policy trajectory (initially identified through primary sources) and instructive, by gaining an understanding of the reasons for policy trajectory, refining research questions and finalising the study's structure.

Summary

Two waves of policy development:

Wright-Neville (2006, p. 1) suggests 'Australia's approach to counter-terrorism has evolved in several waves, each following high-profile terrorist attacks overseas.' A main finding of this study is that Australia's federal critical infrastructure policy has developed in two key waves, following reviews arising from high-profile attacks (one domestic and the other international): these events are the 13 February 1978 bombing outside the Hilton Hotel in Sydney; and the 9/11 terrorist attacks in the USA.

The Hilton Hotel bombing sparked policy responses from the Australian government that included the following: firstly, a Commonwealth police resources review undertaken in 1978 by Sir Robert Mark (the Mark Review); secondly, a wide-ranging Protective Security Review undertaken in 1978 and 1979 by Justice Hope (the PSR Review); and, thirdly, formation of the Standing Advisory Committee on Commonwealth-State Cooperation for Protection Against Violence (SAC-PAV). All would cast long shadows into future CI policy.

The Mark Review led directly to the formation of the Australian Federal Police (AFP), a policing organisation with an enduring and significant role in CI protection in Australia, both through general policing and guarding functions, and involvement in the often complex inter-related governmental committee structures. The PSR Review most directly impacted upon CI policy by leading to establishment of the Vital Installations Program, a forerunner to the Critical Infrastructure Protection Program

of the post-9/11 era. Likewise, the establishment of SAC-PAV - the first multi-jurisdictional committee focused (among other things) on CI protection - provided the basis for the National Counter-Terrorism Committee, announced in the immediate aftermath of the 9/11 attacks.

Not surprisingly, in the period immediately following 9/11 'there was considerable activity by all Commonwealth, State and Territory authorities' (Duckworth, 2007, p. 35). These responses included a review of Australia's counter-terrorism arrangements, conducted by Mr Robert Cornall, Secretary of the Attorney-General's Department (AGD)¹. The impact of the Cornall Review on CI policy included increased resourcing for ASIO, formally ending the so-called ASIO peace dividend of 1992 that had seen its resources significantly reduced. Importantly, Cornall recommended a machinery-of-government change that saw Emergency Management Australia (EMA) transfer from the Department of Defence to AGD to supplement its policy focus. EMA also formally became a member of the NCTC after its formation in 2002. This provided a further institutional vehicle for emergency management policy to influence CI policy. The shift in dominant organising principles of policy impact can be identified in the years that followed, from the earlier terrorism-centric protective security focus, to the later, and broader, all-hazards and resilience focus.

Evolving Definitions:

This study highlights how the definition of CI in Australia has evolved over the past 30 years. In modern policy, the terms used to describe and define Australia's key civil infrastructures, have included "vital installations" and "vital national installations" dominant in the 1980s and 1990s, "lifelines" in the 1990s, and "critical infrastructure" and "designated critical infrastructure", dominant in the post-9/11 period.

During the 1980s and 1990s, the definitional distinction between a "vital installation" and a "vital national installation" had significant policy implications. A "vital national installation" (a so-called super-infrastructure) was a significant policy departure from how "vital installations" were considered,

where the definitional focus was on protection from terrorism, and planning for the protection of Vital National Installations that reflected an "all-hazards" approach. Mr Roger Holdich AM, former Deputy Secretary, Department of the Special Minister of State and former Inspector-General of Intelligence and Security, explained the significant policy implications:

The planning to protect *vital national installations* was what would now be termed the 'all-hazards' approach to contingency planning. It included development of contingency plans for natural and accidental hazards, damage mitigation, alternative supply of products, restoration of supply following loss or impairment of functions and counter-terrorist protective and reactive measures. The planning to protect *vital national installations* was not driven by the threat of a terrorist attack at the time, but by the impact on the Australian people if the particular service was damaged or disrupted².

The terms "vital installations" and "vital national installations" lost policy dominance in the late 1990s with emergence of the term "critical infrastructure." While the term "critical infrastructure" itself has since remained dominant in Australian policy, its definition has proven malleable, although remaining notably and deliberately constant since the mid-2000s. The settled Australian definition of CI is now:

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 wellbeing of the nation or affect Australia's ability to conduct national defence and ensure national security. In this context significant means an event or incident that puts at risk public safety and confidence, threatens our economic security, harms Australia's international competitiveness, or impedes the continuity of government and its services (Commonwealth of Australia, 2010, p. 8).

1 The Cornall review has never been made public.

2 Author interview, 25 July 2011

The concept of “designated critical infrastructure” emerged in 2006 through the *Defence Legislation Amendment (Aid to Civilian Authorities) Act 2006* (Cth). The Act amended the *Defence Act 1903* (Cth) and included the following definitions:

Infrastructure includes physical facilities, supply chains, information technologies and communication networks or systems

Designated critical infrastructure means infrastructure, or a part of infrastructure, that is declared under section 51CB.

These definitions are significant as they create specific legislative powers to protect “designated critical infrastructure” - in particular, the use of lethal force by the Australian Defence Force. The earlier policy concept of “super-infrastructure” has now been reinvigorated and applied to a new era.

Policy Transfer:

With its origin in ‘policy diffusion studies, a sub-set of the comparative politics literature’, policy transfer (PT) is one way of explaining policy change and development (Evans, 2009, p. 244). PT is defined as ‘[how] knowledge about policies, administrative arrangements, institutions and ideas in one political setting (past or present) is used in the development of policies, administrative arrangements, institutions and ideas in another political setting’ (Dolowitz & Marsh, 2000, p. 5). Although not immune from theoretical critique, as a practice,

PT has increasingly become a feature of modern governance, and provides a framework for understanding the often complex ways policy develops and is seen as a ‘rational option for policy-makers’ (Legrand, 2007, p. 16). For PT to occur, it requires a policy feature to be transferred, with potential and motivated agents of transfer including ‘politicians and civil servants ... [and] ... institutions’ (Bulmer, 2007, pp. 48-49).

Drawing from the work of Evans (2009) and Dolowitz & Marsh (2000), key aspects of PT can be summarised as: transfer feature (what is transferred); transfer agent (who transferred); transfer origin (from where did transfer occur); degree of control (voluntary to coercive); and degree of transfer (how much changed in the transfer). The degree of transfer can be assessed via a continuum, a simple scale illustrating the extent to which wholesale PT has occurred (a process continuum). Evans (2009, pp. 245-246) describes this continuum as comprising: *copying* described as where ‘a government organisation adopts a policy, programme or institution without modification’; *emulation* described as where ‘a governmental organization accepts that a policy, programme or institution overseas provides the best standard for designing a policy, programme or institution at home’; *hybridization* described as the most typical form and ‘where a governmental organisation combines elements of programmes found in several settings to develop a policy that is culturally sensitive to the needs of the recipient’; and *inspiration* described as ‘where an idea inspires fresh thinking about a policy

problem and helps to facilitate policy change’.

This study has identified four aspects of the policy trajectory that can be directly attributed to PT in the period 1978 to 2010. From a geo-political perspective, three of these aspects are: formation of the Australian Federal Police and Vital Installations Program, both occurring in 1979; and the precursor to formation of the Trusted Information Sharing Network (TISN) in 1997. From a policy domain perspective, the fourth aspect is emergency management policy, identified as having a significant direct impact on the CI policy trajectory. Through applying specific CI policy attributes to those of PT, a framework was developed to summarise the impact (see Table 1).

Role of Industry:

During 30 years of policy and program development, one of the most significant changes has been the role of industry. From a very low base in 1979 - which included only limited reference to, and role for, industry - the post-9/11 environment shows a policy focus with industry engagement at its core. This policy focus follows privatisation and shift in ownership of assets considered Australia’s CI – in 1979, from predominantly state owned (via the Commonwealth or State and Territory governments) when considered in the PSR Report (giving rise to the Vital Installations Program) - to being predominantly privately owned and operated in the post-9/11 era, when policy was re-examined.

TABLE 1: POLICY TRANSFER FRAMEWORK³

TRANSFER FEATURE	PRIMARY AGENT TYPE	TRANSFER ORIGIN	CONTROL CONTINUUM	PROCESS CONTINUUM
Australian Federal Police	Sir Robert Mark Politicians	UK	Voluntary	Hybridization
Vital Installations Program	Justice Robert Marsden Hope Politicians	UK	Voluntary	Emulation
Trusted Information Sharing Network (including infrastructure categories)	Civil Servants Politicians	USA	Voluntary	Hybridization
Policy	Civil servants Politicians	Emergency management policy	Voluntary	Inspiration

³ This framework has been adapted from the original, see O’Donnell (2011)

Since 9/11, industry engagement has been at the core of CI protection policy. Policy positions such as ‘good security is good for business’, engagement with industry in counter-terrorism exercises, and continued development of the TISN arrangements, demonstrate the centrality of the role of industry and a significant policy shift across the 30 year period. While remaining a core policy goal, the extent to which genuine engagement has been achieved across the diverse range of industry comprising CI warrants further research.

Legislation:

The bombing outside the Hilton Hotel in 1978 and subsequent call-out of armed forces in the so-called ‘Siege of Bowral’ was identified by the Australian Government at that time as highlighting Australia’s ‘relative unpreparedness, in an administrative and legislative sense, for terrorist events (Commonwealth of Australia, 2002, p. 1). In this context, preparedness in the legislative sense related to the constitutional framework of the relationship between the Defence Force and civil authorities in respect of civilian security, including ‘provisions of the Defence Act and of the regulations and administrative instructions issued under it’ (Commonwealth of Australia,

1979a, p. 140). Given the CI policy context at the time - where even Australia’s defence-focused Vital Points Program had lapsed and the Vital Installations Program had not yet formed - that this was the legislative focus is unremarkable. What is noteworthy is that, despite the rise and rise of administrative policy focused on protecting CI since then, the sole federal legislation specifically focused on protecting CI NSI relates to Part IIIAAA provisions of the *Defence Act 1903* (Cth), and more particularly the 2006 amendments. This is despite the 9/11 terrorist attacks that initiated and so heavily influenced administrative policy arrangements, a range of options available under the Constitution, and the model provided by the *Terrorism (Community Protection) Act 2003* (Vic) also considered by Tasmania. Rather, administrative policy still remains dominant.

Summary:

In identifying and analysing key aspects of federal policy focused on CI over a 30 year period, this study sought to explain how and why policy developed in the way it did. It examined how the key influencing factors of PT, the changing role of industry, and role and focus of legislation, impacted upon the policy trajectory. The following framework situates the key

policy factors and eras identified in this study, and summarises the key findings (see Table 2).

Further Research:

With a focus on federal CI policy and bounded by the period 1978 – 2010, this study has considered only part of the CI policy trajectory in Australia. With the constitutional role of State and Territory Governments, and the role of owners and operators of CI, significant further research is needed to complete the analysis and reveal policy trajectory within this broader context. Variations in policy and arrangements across sectors comprising Australia’s CI remains unexplored, as does the dual role of the State in being both *regulator* and *owner and operator* of some CI. Research into the development of CI policy in Australia pre-1978 would likewise enrich the policy picture, in particular, how the Australian government considered the defence of CI in World War I and World War II. Further research could explore how Australia’s CT policy was drawn from the UK prior to 1978 and, given its significance in the formation of Australia’s Vital Installations Program, how the UK’s Vital Points Program operated.

TABLE 2: SUMMARY OF FACTORS IMPACTING CRITICAL INFRASTRUCTURE POLICY⁴

FACTORS	ERA 1 1978 – 1991	ERA 2 1992 – Pre-9/11	ERA 3 Post-9/11
Trigger Events	Domestic: Hilton Hotel bombing Sydney	Domestic: Incursion Iranian Embassy Canberra	International: 9/11 terrorist attacks
Key Reviews	Mark (1978) Hope (1978 – 79) Holdich (1986)	Codd (1992) SAC-PAV (1993)	Cornall (2001) CIP Review Team (2007) Smith (2008) COAG Senior Officials (2009)
Terms and Definitions	Key Points Vulnerable Points Vital Points Vital Installations Vital National Installations	Vital Installations Vital National Installations Lifelines Critical Infrastructure	Critical Infrastructure Critical Physical Infrastructure Designated Critical Infrastructure
Key Government Decisions and Policy Focus	AFP Vital Installations Program SAC-PAV	Tasmanian Lifelines Project Pre-TISN ASIO ‘Peace Dividend’ Y2K Sydney Olympics	Business-Government Task Force TISN NCTC “Good security is good for business”
Industry Engagement	Limited	Evident	Structured and formalised
NSI Legislation	Treaty driven (dominant)	Treaty driven (evident)	<i>Defence Legislation Amendment (Aid to Civilian Authorities) Act 2000</i> (Cth) <i>Defence Legislation Amendment (Aid to Civilian Authorities) Act 2006</i> (Cth)
Policy Transfer	Evident	Evident	Institutional vehicles evident

⁴ Adapted from original, see O’Donnell (2011)

References

- Bulmer, S. (2007). Germany, Britain and the European Union: Convergence through Policy Transfer? *German Politics*, 16(1), 39-57.
- Commonwealth of Australia. (1979). *Protective Security Review Report (confidential version)*. Canberra: Australian Government Publishing Service.
- Commonwealth of Australia. (1979a). *Protective Security Review (unclassified version)*. Canberra: Australian Government Publishing Service.
- Commonwealth of Australia. (2002). *Attorney-General's Department Annual Report 2001-02*. Canberra: Attorney-General's Department.
- Commonwealth of Australia. (2010). *Critical Infrastructure Resilience Strategy*. Canberra: Attorney General's Department.
- Dolowitz, D., & Marsh, D. (1996). Who Learns What from Whom: a Review of the Policy Transfer Literature. *Political Studies*, XLIV, 343-357.
- Dolowitz, D., & Marsh, D. (2000). Learning from Abroad: The Role of Policy Transfer in Contemporary Policy-Making. *Governance: An International Journal of Policy and Administration*, 13(1), 5-24.
- Duckworth, M. (2007). Developing the Victorian Policy and Legislative Approach to Counter-Terrorism. *Counter-Terrorism International Conference 2007* (pp. 35-40). Melbourne: Victoria Police and Monash University.
- Evans, M. (2009). Policy transfer in critical perspective. *Policy Studies*, 30(3), 243-268.
- Legrand, T. (2007) *Overseas and Over Here: The Politics and Pathways of Policy Transfer*, PhD thesis, University of Birmingham.
- O'Donnell, K. (2011) *From guns, gates and guards: the development of Australia's federal critical infrastructure policy, 1978 – 2010*, Masters (Honours) thesis, Griffith University.
- Wright-Neville, D. (2006). The Politics of Fear: Counter-Terrorism and Australian Democracy. Working Paper (WP) 27/2006. *Real Instituto Elcano*, 1-14.

Legislation

Defence Act 1903 (Cth)

Defence Legislation Amendment (Aid to Civilian Authorities) Act 2006 (Cth)

Terrorism (Community Protection) Act 2003 (Vic)

Interview

Holdich, R. (2011, July 25). Former Deputy Secretary, Department of the Special Minister of State, and former Inspector-General of Intelligence and Security. (K. O'Donnell, Interviewer) Canberra.

About the Author

During 2011 and as a Senior Officer with the Department of Transport and Main Roads, Kate O'Donnell was seconded for 12 months to the position of Practitioner-in-Residence with the Australian Research Council Centre of Excellence in Policing and Security (CEPS) headquartered at Griffith University. While at CEPS Kate's key focus has been to work with the CEPS researchers to bring a transport security focus to the research program and to work to build strong linkages with CEPS and the transport sector. While at CEPS Kate completed the Master of Criminology and Criminal Justice (Honours) Program with research focused on the development of Australia's critical infrastructure protection policy and arrangements. Into the future, Kate continues her association with Griffith University and CEPS and Griffith University through the PhD program. Kate can be contacted at k.odonnell@griffith.edu.au.

ARC Centre of Excellence in Policing and Security

M10_3.01
Mt Gravatt Campus
170 Kessels Road
NATHAN QLD 4122
Ph: 07 3735 6903
Fax: 07 3735 1033

www.ceps.edu.au



Australian Government
Australian Research Council



**Australian
National
University**



**THE UNIVERSITY
OF QUEENSLAND**
AUSTRALIA



**Charles Sturt
University**

Views expressed are personal to the author, and should not be attributed to CEPS or its industry partners.