Research Article

CRITICAL INFRASTRUCTURE RESILIENCE: RESILIENCE THINKING IN AUSTRALIA'S FEDERAL CRITICAL INFRASTRUCTURE PROTECTION POLICY

Kate O'Donnell[†]

Australia's national security policy is set out in a number of complex and interrelated policy documents that span multiple agencies, impact all levels of government (federal, state and local) and require strong partnerships with the private sector. This study examines the emergence of the term and concept of critical infrastructure (CI) in modern policy and its development in Australia's national security policy. Since its emergence in Australian federal policy, the term *CI* has evolved and stabilised. Yet, in the last decade CI policy has expanded to incorporate *resilience thinking* and the concept of *critical infrastructure resilience* (CIR) is now at the core of Australia's federal CI policy. This study identifies the emergence and development of federal policy focused on protecting Australia's most vital assets in peacetime. In doing so, it highlights that in Australian federal policy, CIR has been conceptualised in four distinct ways. However, *resilience* as a body of knowledge is still evolving. Articulating and analysing how resilience thinking has been incorporated into Australia's federal CI policy, is an important next step in assessing policy focused on the protection Australia's most vital and iconic assets.

Keywords: counterterrorism; critical infrastructure; infrastructure protection; resilience; policy

INTRODUCTION

With its genesis in the United States (US) in 1980s, the term *critical infrastructure* (CI) is now firmly part of the modern scholarly, political and policy lexicon (see for example Brown, 2006; Commonwealth of Australia,

[†] Corresponding author: k.odonnell@griffith.edu.au

2010a; Department of Homeland Security, 2009; Moteff & Parfomak, 2004; Rudd, 2008). While now a settled concept broadly referring to essential services and their networks and supply chains that support national security, economic prosperity and social and community well-being, conceptualising and defining what does (and does not) fit within the rubric of CI has developed and evolved. While it had been used in the 1980s, the term CI was cemented in the US policy discourse in the 1990s through the US Government's response to the 1995 bombing of the Alfred P Murrah Federal Building in Oklahoma City (Brown, 2006).

The term jumped the Pacific soon afterwards, and by 1997 had tentatively entered the Australian policy discourse, although without the clarity it later gained in the wake of the 9/11 terrorist attacks (O'Donnell, 2011). The Australian Government's response to the 9/11 terrorist attacks included an immediate political and policy focus on protecting CI (Business Government Taskforce on Critical Infrastructure, 2002; Protective Security Coordination Centre, 2002). This response built on the arrangements that had been put in place to protect key civil infrastructures in peacetime through the Vital Installations (VI) Program of the 1980s and 1990s. In the decade since 9/11, Australia's federal policy focus on CI has been sustained yet has developed and evolved (O'Donnell, 2011).

While there is reasonable international consensus on the concepts and definitions of CI, the concepts and definition of *critical infrastructure resilience* (CIR) remain malleable and under development. Reflecting the multi-disciplinary nature of scholarly and policy attention, it is perhaps unsurprising that CIR itself has been conceptualised differently by scholars and policymakers alike. In this article, the emergence of the term CI in the US and its adoption into, and development within, Australian federal policy is firstly identified.

The concept of *resilience* and how it became a key plank of Australia's CI protection policy is then examined. Through this analysis, it is clear that in Australian federal policy, four distinct ways of conceptualising CIR are evident. This has important implications for how the still evolving and developing concepts of resilience can be considered and incorporated into future policy. Within the Australian federal policy framework, CIR has been conceptualised in the following ways: as a policy concept; as a business model (organisational resilience); as cyber systems; and as engineering design and strategic asset

management. In policy terms, this evolved from an earlier concept of protecting CI from terrorism in peacetime.

EMERGENCE OF THE TERM CRITICAL INFRASTRUCTURE

In detailing the development of CI protection arrangements in the US, Brown (2006, p. ix) notes that 'since the American Revolution, our greatest leaders have recognized that a key indicator of national strength is the development and maintenance of an advanced system of infrastructures'. In chronicling the development of policy and arrangements focused on protecting such assets from the 1790s, through the Great War, World War II and the Cold War, and into the post-Cold War environment, Brown (2006) establishes that it is the *term CI* and not the *concept of CI* that is new to modern policy. However, there remains debate about exactly when the term CI was coined.

While Brown (2006, p. 71) suggests that the term CI itself was first used in 1989 in a report presented to the US Senate Committee on Governmental Affairs that focused on infrastructure issues, Moteff & Parfomak (2004, p. 4) suggest it appeared in the US earlier in the same decade 'in some form in many of the policy debates in the 1980s'. Nevertheless, the term itself had emerged in the policy discourse, however its meaning and definition remained somewhat elusive into the mid-1990s in the US, and into the post 9/11 era in Australia.

As part of the US government's policy response to the April 1995 bombing of the Alfred P Murrah Federal Building in Oklahoma City, then President Clinton signed Presidential Decision Directive 39 (PDD 39), US Policy on Counterterrorism (Brown, 2006, pp. 71-72; The White House, 1995). Importantly, while the PDD 39 uses the term *critical national infrastructure*, an examination of its unclassified version offers little in the way of concepts or definitions of what may (or may not) have been specifically considered critical national infrastructure at the time (The White House, 1995). The PDD 39, did however, lead to the establishment of the Critical Infrastructure Working Group (CIWG). (Note that only part of PDD 39 has been made public.)

Reporting in 1996, the CIWG made two principle recommendations: the establishment of a group within the Federal Bureau of Investigation to 'keep an eye on infrastructure issues for the short term' and the establishment of "a full-time Presidential Commission devoted to looking at critical infrastructure" (Brown, 2006, p. 78). In July 1996, through Executive Order 13010, then President Clinton further instructed the establishment of a President's

Commission on Critical Infrastructure Protection (the Commission) (The White House, 1996). Executive Order 13010 described CI in the following way:

> Certain national infrastructures are so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States. These critical infrastructures include telecommunications, electrical power systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems, emergency services (including medical, police, fire, and rescue), and continuity of government. Threats to these critical infrastructures fall into two categories: physical threats to tangible property (''physical threats''), and threats of electronic, radio-frequency, or computer-based attacks on the information or communications components that control critical infrastructures (''cyber threats'') (The White House, 1996, p. 1).

Over fifteen months, the Commission Chaired by General Robert T Marsh, considered the protection of CI in the US and reported to the President on its findings and conclusions in October 1997 (President's Commission on Critical Infrastructure Protection, 1997). Marsh reflected on the enormity of the task of the Commission, and in particular the challenges posed by conceptualising, defining and identifying CI: he specifically noted "one of the greatest challenges was: What is this infrastructure?" (Marsh cited in Brown, 2006, p. 98). More specifically, during the Commission's considerations, a fundamental question was posed that provides rich insights into how the Commission was grappling with conceptualising CI, "(w)e talk about this critical infrastructure but do we know what we're talking about?" (Marsh cited in Brown, 2006, p. 98). Therefore, it can be concluded that while the term CI had entered the policy lexicon of the US almost a decade previously, its precise technical and practical meaning remained somewhat elusive well into the 1990s. As part of the Commission's report, a clear definition of CI was articulated and was settled in the following way:

> Critical Infrastructures: Infrastructures that are so vital that their incapacitation or destruction would have a debilitating impact on defense or economic security (President's Commission on Critical Infrastructure Protection, 1997, pp. B-1).

CRITICAL INFRASTRUCTURE IN THE AUSTRALIAN POLICY CONTEXT

As US policymakers grappled with conceptualising and defining the term CI in the 1990s, it was used in Australia as part of the Tasmanian Lifelines Project, an emergency management focused project with the goal of identifying and protecting key parts of the State of Tasmania's civil infrastructure in peacetime (O'Donnell, 2011; Tasmanian Government, 1997). As in the US, although the term CI was "new", the concept had a longer pedigree. In the Australian context, the antecedents of a formal federal policy and structured program focused on the protection of key civil infrastructures in peacetime rests with the VI Program of the 1980s and 1990s and the terms "vital installations" and "vital national installations". The genesis of this program was the response to the bombing outside the Hilton Hotel in Sydney on 13 February 1978.

As part of the Australian government's policy response to the bombing, then Prime Minister Fraser appointed Justice Robert Marsden Hope to conduct a wide ranging protective security review (Commonwealth of Australia, 1979a). In his report, Justice Hope gave specific thought to how Australia's key civil infrastructures could be protected in peacetime and distinguished between key civil infrastructures (that he termed *vital points*) and key defence infrastructures (that he termed *key points*) (Commonwealth of Australia, 1979b, pp. 150-155). While a clear definition *per se* is not evident in the report, "vital points" were described in the following ways:

> . . . installations whose unimpeded operation is necessary for the orderly life of the community . . .
>
> . . . installations upon which the well-being and orderly life of modern industrial cities depend. They include power stations, water supply pumping stations, petroleum refineries, offshore oilrigs, natural gas pipelines and computer installations (Commonwealth of Australia, 1979b, p. 151).

Although Justice Hope recommended Australia develop a Vital Points Program to protect Australia's key civil infrastructures in peacetime, it was the term *vital installations* that was adopted in Australia through the establishment in the 1980s of the VI Program (O'Donnell, 2011). In particular, the VI Program was designed for the identification and protection of 'important parts of the civil infrastructure' from terrorism (Sheldrick, 1986, p. 512). Mr John Lines, who

was a member of the Counter-Terrorism Branch of the Protective Security Coordination Centre, (1978–1992) explained that the VI Program was established in September 1980 coming on line by early 1981 (J. Lines, personal communication, May 2013). Its focus was infrastructure assets that were significant, but not necessarily from a military perspective (J. Lines, personal communication, May 2013). As part of the VI Program, there were two tiers of civil infrastructures: Vital Installations and Vital National Installations. They were distinguished in the following way:

> A Vital Installation (VI) is a facility, installation or resource, the loss of the products or services of which would severely disrupt the orderly life of the community, or which, if damaged, would cause a major public hazard.
>
> A Vital National Installation (VNI) is a vital installation in which the Commonwealth and one or more State/Territory Governments have substantial interests and responsibilities, and/or the installation is of major national economic importance (Sheldrick, 1986, p. 516).

While the term CI had tentatively formed part of Australian policy since the 1990s, co-existing with VI and VNI, it gained dominance in the post-9/11 era. The immediate policy response by the Australian government to the 9/11 attacks included an announcement on 7 November 2001, by the then prime minister, Mr John Howard, of his intention to form a Business Government Taskforce on Critical Infrastructure to give business greater input into the assessment of current arrangements to protect national infrastructure (Business Government Taskforce on Critical Infrastructure, 2002). A key document of the time identifies that key civil infrastructure was termed *critical physical infrastructure*, and was described by the Australian Government (Protective Security Coordination Centre, 2002, p. 8) as including:

- institutions, such as official establishments, key foreign missions/residences, Federal and State Houses of Parliament, and key Commonwealth government departments and military facilities;
- financial infrastructure, such as banking and stock exchanges;
- economic infrastructure, such as the NW Shelf oil and gas fields;
- other important facilities, such as the Lucas Heights nuclear reactor;
- public utilities, such as energy and water supply;
- logistic infrastructure, such as roads, bridges, rail and ports;

- Australian symbols, such as the Sydney Opera House and Harbour Bridge, Australian War Memorial, prominent city buildings and major sporting facilities; and
- some elements of the National Information Infrastructure, such as the crucial telecommunications facilities, which also require protection from physical threats.

This highlights that in Australia, the very concept of *criticality* of infrastructure underpinning the earlier VI Program was reconsidered by the Protective Security Coordination Centre in the immediate aftermath of the 9/11 terrorist attacks. The way critical physical infrastructure was considered, expanded to incorporate Australian symbols as well as core infrastructure types, such as utilities and transport. Since then, while the concept and definition of CI evolved, its definition has remained notably and deliberately constant in Australian federal policy since the mid-2000s (O'Donnell, 2012). The Commonwealth, and State and Territory governments have agreed to define CI in the following way:

> ...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, 2010a, p. 8).

The shift to this definition of CI, signals a maturing of policy to one that conveys broad concepts of *criticality* of infrastructure without limiting the source or nature of threat to that infrastructure, and without limiting infrastructure types. This definition does, however, belie the complexity of networked and interdependent sectors and systems that collectively comprise Australia's CI. This complexity is partly identifiable through the construct of the Trusted Information Sharing Network (TISN) that comprises seven sector groups (banking and finance; communications, energy, food chain, health, transport, and water services), two expert advisory groups (resilience and information technology security), one oil and gas security forum and various issues-driven communities of interest (Trusted Information Sharing Network, n.d.).

WHAT IS CRITICAL INFRASTRUCTURE RESILIENCE?

Having settled the concept and definition of CI, what then is CIR? While the term CIR is cemented in the Australian CI policy, its concept and definition is diverse both internationally and within Australia. The meaning of resilience itself varies to the extent it has become somewhat of a catch-all term (Gibson & Tarrant, 2010; McAslan, 2010a, 2010b; Ridley, 2011). McAslan (2010a) identifies the long and rich history of the term and concept of resilience noting its introduction into the English language in the Seventeenth Century, its use in the nineteenth century in materials science and its much later introduction to ecology and the environment.

In describing the origin, meaning, and evolution of the term and concept of resilience, McAslan (2010a, p. 1) also notes the term itself has, in less than a decade, "evolved from the disciplines of materials science and environmental studies to become a concept used liberally and enthusiastically by policy makers, practitioners and academics." Its adoption and integration in federal CI policy in Australia is no exception (see for example Commonwealth of Australia, 2010a; Commonwealth of Australia, 2010b).

As Kendra and Wachtendorf (2003, p. 41) identify, "defining resilience is clearly challenging." Defining *resilient infrastructure* offers a further challenge. Boone and Hart (2012) note the proliferation of both literature and policy related to CIR and identify the complexity and difficulty in linking individual works to the broader body of knowledge. Noting the inherent difficulties in capturing CIR as a field of work, and drawing from military concepts, they set out, in respect of CI, the concept of *full spectrum resilience* (FSR): an organising principle "which relates individual elements of critical infrastructure work and scholarship to each other and to the body as a whole" (Boone & Hart, 2012, p. 4).

The concept of FSR has been designed as a form of classification to make sense of the range of "scholarship, research, publications, codes and standards for protection into a coherent whole" (Boone & Hart, 2012, p. 6). It makes a significant contribution to both scholarship and practice. FSR comprises three aspects: levels of resilience (strategic, operational and tactical); range of impact (national, regional, community, individual); and the all hazards environment (terrorism, accident, earth effect and deterioration) and offers one way of classifying and analysing CIR related policies and programs within a matrix of forty-eight different categories (Boone & Hart, 2012, pp. 5-6). In doing so, it

offers a practical way of articulating the focus and limits of specific policies and programs, how policies and programs can or should relate to each other, and a mechanism for assessing gaps in policies and programs (Boone & Hart, 2012, p. 6). While the focus of FSR is "establish a coherent framework for thinking about all related aspects of resilience and the body of knowledge as a whole," its architects also identify that it should not limit creative thought (Boone & Hart, 2012, p. 6).

While individual policies and programs can be mapped within the matrix of FSR, within Australian federal policy, CIR has been conceptualised in four specific ways that risk being lost in the FSR matrix. In particular, in Australian federal policy, CIR has evolved and been conceptualised as: a policy concept; as a business model (organisational resilience); as cyber systems; and as engineering design and strategic asset management. Understanding the very different ways critical infrastructure resilience has been conceptualised in Australian policy will provide a stronger basis for policy analysis and evaluation.

1—Policy Concept

The adoption of CIR as a dominant policy concept in the Australian Government's CI protection arrangements can be considered evolutionary, that shifted from a specific focus on terrorism to one incorporating consideration of broader threats and hazards. The practical impact of this is that for a broader range of infrastructures, a broader range of threats have been incorporated into the policy framework. Two policy concepts were at the core of the Australian VI Program of the 1980s and 1990s: a focus on terrorism that applied to VIs, and a broader focus on disruptions that applied to VNIs. The focus of the VI Program was on identifying and ensuring 'adequate protective and contingency measures for installations in the program' (Sheldrick, 1986, p. 518). Mr Roger Holdich, AM, who was formerly Deputy Secretary, Department of the Special Minister of State, and formerly Inspector-General of Intelligence and Security, described how the two policy concepts co-existed within the VI Program:

> [by 1986] Australia's counter-terrorism arrangements were primarily focused around prevention and protection measures.
>
> 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 (R. Holdich, personal communication, July 25, 2011).

In 1986, Mr Holdich, at the direction of the then Special Minister of State, conducted a review of Australia's counterterrorism capabilities. His report has never been released publicly.

The VI Program had effectively lapsed by the time of the 9/11 terrorist attacks that drew a significant and sustained policy response from the Australian government focused on CI protection (O'Donnell, 2011). The multi-pronged policy response to 9/11 included the formalisation and enhancement of a structured government and industry consultation forum in the form of the TISN that built on earlier arrangements. Mr Mike Rothery, who is First Assistant Secretary, National Security Resilience Policy Division, Attorney-General's Department, explained that the policy response also included the establishment of the CI Protection Program in 2003 that would, from the outset, take a focus beyond terrorism to include CI protection in the face of increasing risks and hazards (M. Rothery, personal communication, November 1, 2012). Mr Rothery has also clarified the development of, and at times subtle differences in policy concepts:

> The decision to form the TISN was taken by Cabinet and arose from the recommendations of the Business Government Taskforce that met in 2002. Built into the TISN model approved by Cabinet was an 'all hazards' focus.
>
> In parallel, [the Council of Australian Governments] changed the National Counter-Terrorism Committee to examine [critical infrastructure protection] from a counter-terrorism focus, which naturally focussed on the identification and protection of assets.
>
> The TISN has, since its inception, has taken an 'all-hazards' approach albeit with an initial focus on counter-terrorism. However, in recent years there has been a rebalancing/refocusing towards 'resilience.' The decision in recent years to 'drop the P' in Critical Infrastructure Protection and rename the program Critical Infrastructure Resilience was a deliberate move to ensure there was a differentiation from 'guns gates and guards' (M. Rothery, personal communication, June 30, 2011).

In the years leading up to 2009 when the Attorney-General publically announced the Australian Government's intention to shift the CI Protection Program to a resilience footing, Australia's federal CI policy continued to further incorporate

resilience thinking. This is seen through the formation in 2007 of the TISN Resilience Community of Interest, the 2007 review of the Australian Government's CI Protection Program that recommended the program shift to a focus on resilience, the 2008 review of Australia's homeland and border security arrangements that noted resilience was a feature of CI policy and should be promoted, and the 2009 review of CI protection arrangements that identified limitations in a singular focus on either counterterrorism or all-hazards (Commonwealth of Australia, 2010a). In 2010 and in directly articulating resilience as an overarching goal, the Australian Government released its *Critical Infrastructure Resilience Strategy*, that linked CI to resilience in the following way:

> The aim of this Strategy is the continued operation of critical infrastructure in the face of all hazards, as this critical infrastructure supports Australia's national defence and national security, and underpins our economic prosperity and social well-being. More resilient critical infrastructure will also help to achieve the continued provision of essential services to the community. . . .
>
> It is important to note that some elements of critical infrastructure are not assets, but are in fact networks or supply chains. For example, bringing food from the paddock to the plate is dependent not only on particular key facilities, but also on a complex network of producers, processors, manufacturers, distributors and retailers and the infrastructure supporting them. In the context of critical infrastructure, resilience refers to:
>
> - coordinated planning across sectors and networks;
> - responsive, flexible and timely recovery measures; and
> - the development of an organisational culture that has the ability to provide a minimum level of service during interruptions, emergencies and disasters, and return to full operations quickly.
>
> In this way, building capacity in organisations to be agile, adaptive and to improve by learning from experience is part of the concept of CIR. (Commonwealth of Australia, 2010a, p. 8).

It is evident then, that CIR as a policy concept draws from the all-hazards policy concept and the concept of *organisational resilience*. Incorporating organisational resilience as part of the CIR policy concept extends the policy reach because of its clear impact on the owners and operators of CI assets.

2—Business Model (Organisational Resilience)

At the time the Vital Points Program was proposed by Justice Hope in 1979, the majority of key civil infrastructures were owned and operated by the state (either the federal or state and territory governments) (Commonwealth of Australia, 1979a; O'Donnell, 2011). However, the 1980s and 1990s saw a shift in ownership of key civil infrastructure assets to the private sector (such as telecommunications, energy, transportation and banking) to the extent that the majority of CI in Australia is now privately owned, or operated on a commercial basis (Commonwealth of Australia, 2010a; Rudd, 2008). The influence of the shift in ownership and operation of CI assets from the state to the private sector is clearly seen through the emergence and adoption of a policy focus that includes organisational resilience and promotion of the concept that "good security is good for business"(see for example Commonwealth of Australia, 2007, 2010a, 2010b, 2011, 2012b).

McAslan (2010b) argues the concept of organisational resilience itself is relatively new, emerging in 2003 as a management concept. However, in much the same way Brown (2006) identifies the *term* CI and not the *concept* of CI emerged in the 1980s, Kendra and Wachtendorf (2003) artfully analyse the rich seam of earlier organisational literature on which concepts of organisational resilience draw. While a precise definition of organisational resilience has not been settled, clarity is being pursued through the development of an International Organisation for Standardisation (ISO) standard for organisational resilience based on the *Organizational Resilience: Security, Preparedness and Continuity Management Systems* standard developed in 2009 by ASIS International (McAslan, 2010a).

In noting the complexity of the concept of organisational resilience, McAslan (2010b, p. 1), describes it as the "ability of organisations to recover and return to normality after facing an alarming and often unexpected threat' and notes (2010b, p. 15) there remains some confusion on how best to apply the concept in a reliable and consistent manner." Gibson and Tarrant (2010, p. 6) view organisational resilience as complex and multi-dimensional, more than simply an organisation's ability to bounce back from adversity, as being founded in the understanding and treatment of risk and vulnerabilities, and something able to be conceptualised in a variety of ways.

Since its emergence as a term and concept, organisational resilience, has gained policy momentum to the extent of its formal adoption into Australian national security policy, in particular as part of CI policy and disaster management policy (see for example Commonwealth of Australia, 2010a, 2010b; Council of Australian Governments, 2011). Further, the construct of organisational resilience as a key part of the business model for CI assets, was formally endorsed as part of the Australian Government's *Critical Infrastructure Resilience Strategy* to 'help achieve the resilience of critical infrastruture in the face of unforeseen or unexpected hazards' (Commonwealth of Australia, 2010a, p. 12). It placed responsibility on achieving resilience with the owners and operators of CI by encouraging a business model that incorporates a focus on organisational resilience. It further identified the need to "promote a common understanding of, and body of knowledge about, organisational resilience" and in pursuit of this, has released a range of policy support documents (Commonwealth of Australia, 2011, p. 1).

The Australian Government recognises that organisational resilience is complex, is one aspect of the broader construct of resilience and means different things to different people (Commonwealth of Australia, 2011, p. 2). Within this policy context, the onus is broadly placed on businesses to pursue organisational resilience and to adopt management strategies to suit the individual business needs.

3—Cyber Systems

As noted, in Australia's federal policy context, the concepts and definitions of CI shifted over time from a specific focus on physical assets to include information technologies and communication networks. The policy frameworks for both CI as physical assets and CI as information infrastructure essentially developed simultaneously and have converged to the extent that achieving the overarching objectives of the 2010 *Critical Infrastructure Resilience Strategy* is reliant on resilient networked systems.

In 1997, as the term CI was tentatively used in Australian emergency management policy discourse, the Australian Government was considering measures to protect Australia's national information infrastructure (NII), noting that information networks were at the core of Australia's "political, strategic and socio-economic well-being" (Attorney-General's Department, 1998, p. 1). In August 1997, Australia's Secretaries' Committee on National Security

considered *Australia's National Information Infrastructure: Threats and Vulnerabilities*, a classified report prepared by the Defence Signals Directorate (DSD) earlier that year that focused on information infrastructure (a grouping of information and communications systems) which at the time was distinguished from physical infrastructure (Attorney-General's Department, 1998).

While the Australian Government did, at the time, note that the US took a broader view and considered both physical and cyber systems in what it considered CI, its focus did include an all-hazards approach to the protection of the NII (Attorney-General's Department, 1998, p. 8). Importantly, DSD identified key industry groupings relevant to the NII (telecommunications, banking and finance, transportation, energy, water supply, information services and emergency services), essentially the same industry groups as those identified under the broader CI policy (Attorney-General's Department, 1998). Mr Ian Carnell, who was formerly the Deputy-Secretary Attorney-General's Department and former Inspector-General of Intelligence and Security, explained that the growing policy focus on NII in the 1990s:

> In the 1990s, the security focus was increasingly on e-crime, cyber-vulnerabilities and IT system security. The lead up to Y2K helped bring this to the fore and this focus from a policy perspective was supported by the Defence Signals Directorate (I. Carnell, personal communication, July 13, 2011).

At the same time, Australian policymakers were taking a policy cue from the US and their focus on CI and information infrastructure. Mr Peter Ford, who was formerly the First Assistant Secretary, Information and Security Law Division, Attorney-General's Department, explained how this occurred:

> In around 1997 I met with a visiting US delegation from the State Department. The US delegation suggested that bilateral engagement on what they described as the protection of critical information infrastructure would be valuable. The US delegation described the consultative arrangements in place with government and owners and operators of critical information infrastructure in the US.
>
> I reported on the talks with the US Delegation to the Attorney-General and recommended that Australia set up a somewhat similar consultative arrangement with the owners and operators of critical infrastructure. At the time, a key focus at the time was on critical infrastructure which was considered to be telecommunications, essential government services, public

> utilities, transport services and food distribution. The Attorney-General agreed (P. Ford, personal communication, July 25, 2011).

Since then, the complex networked systems that underpin CI have continued to gain policy attention to the extent that cyber security forms an integral part of the overall CIR structure and arrangements. This is particularly evident in the ongoing work of CERT Australia (Australia's national computer emergency response team), the IT Expert Advisory Group formed as part of the TISN structure, the 2009 *Cyber Security Strategy* and the 2010 *Achieving IT Resilience: Summary Report for CIOs and CSOs* (see Commonwealth of Australia, 2009, 2012a; TISN for Critical Infrastructure Resilience, 2004; Trusted Information Sharing Network for Critical Infrastructre Protection, 2010).

4—Engineering Design and Strategic Asset Management

McAslan (2010a, p. 2), identifies that while the term *resilience* entered the English language in the Seventeenth Century, it first appeared in scholarly work in 1818 as a term describing the rebound properties of timber. From this beginning, it gained further traction in the mid-eighteenth century through the concept of the modulus of resilience, 'a means of assessing the ability of materials to withstand severe weather conditions' later adopted by the UK's Institute of Civil Engineers (McAslan, 2010a, p. 2). By the late-eighteenth century, resilience was formally defined as:

> a measure of a material to withstand impact, for if a shock or sudden blow be produced by a falling body, its intensity depends upon the weight and the height through which it has fallen, that is, upon its kinetic energy or work. Hence the higher resilience of a material the greater its capacity to endure work that may be performed upon it. The modulus of resilience is a measure of this capacity within the elastic limits only' (Merriman 1885 cited in McAslan, 2010a).

In the twenty-first century, the modulus of resilience remains part of design codes used by civil and mechanical engineers as well as naval architects (McAslan, 2010a, p. 2). While significant technical and scholarly thought has been given over to resilience in the engineering and design fields and in terms of strategic asset management, it is noteworthy that within Australian federal CI policy does not specifically integrate it within the CIR policy framework. Rather, in the Australian federal CI policy context, resilience in terms of engineering design and strategic asset management is seen as an outcome (M. Rothery, personal communication, November 1, 2012).

As a result, in policy the onus rests with owners and operators of CI to ensure that relevant engineering and technical design and asset management meets relevant corporate needs and risk profiles (M. Rothery, personal communication, November 1, 2012). That one of the key success criteria of the *Critical Infrastructure Resilience Strategy* (Commonwealth of Australia, 2010a, p. 26) is "the need for investment in resilient, robust infrastructure being considered in market regulation decisions," reinforces the subtlety in how CIR has been conceptualised in terms of engineering design and strategic asset management and therefore drawn within the policy framework. Within this policy context, Yates (2003) identifies the contribution the discipline of engineering can make to the protection of CI in Australia.

SUMMARY AND FURTHER RESEARCH

Since entering the policy discourse in the 1980s in the US and the 1990s in Australia, the definition of CI has evolved and developed. In Australia the definition of CI has been stable since the mid-2000s. We collectively know what we are talking about when we talk about CI. While this is the case for CI, it can be concluded that the same is not true for how scholars and policymakers alike have considered resilience and its application to CI policy both in Australia and internationally. As identified, concepts of resilience and critical infrastructure resilience are still evolving. Applying concepts of resilience to infrastructure protection has seen the emergence in Australian federal policy of four distinct yet interrelated ways of conceptualising resilient infrastructure. Considered separately, no one conceptualisation is complete and can achieve the policy intent of "achieving resilient critical infrastructure."

While *prima facie* the conceptualisations appear disparate, they are on close analysis wholly interdependent. In the absence of legislation or regulation mandating approaches to protection and recovery across all the CI sectors, the policy intent of "achieving resilient critical infrastructure" can only be achieved through the government working with the owners and operators of CI. In Australia, the majority of CI is privately owned or operated on a commercial basis.

The policy goal of "achieving resilient critical infrastructure" is then in turn dependent on these diverse privately-owned and operated businesses individually embracing both organisational resilience (in terms of business models), and management of the physical infrastructures (in terms of effective

engineering design and strategic asset management). Individual infrastructures are then in turn supported by, and dependent on, robust cyber systems that provide both business and infrastructure enabling functions. While FSR offers a significant contribution to connecting resilience thinking in terms of CIR policy, in Australia it should be approached with caution. This is because it is underpinned by an assumption that the concept of resilience and its application to CI is settled. What the Australian situation demonstrates this is far from the case.

By drawing on its historical context, this paper sets out one way in which federal critical infrastructure resilience policy can be better understood and analysed in the Australian context. By identifying the ways in which "resilience thinking" has been incorporated into policy, it also provides a lens through which future policy change can be assessed and evaluated. However, the ways in which Australian states and territories have conceptualised and embodied resilience thinking within their respective policy frameworks remains under researched. It is only through extending research into these policy areas that a more complete picture of how critical infrastructure resilience has been conceptualised in Australia will emerge.

REFERENCES

Attorney-General's Department. (1998). *Protecting Australia's National Information Infrastructure: Report of the Interdepartmental Committee on Protection of the National Information Infrastructure* Canberra: Attorney-General's Department.

Boone, E. W., & Hart, S. D. (2012). Full Spectrum Resilience: An Executive Summary. *The CIP Report 10*(12), 24.

Brown, K. A. (2006). *A Brief History of Critical Infrastructure Protection in the United States*. Fairfax: Spectrum Publishing Group, Inc.

Business Government Taskforce on Critical Infrastructure. (2002). *Business-Government Taskforce on Critical Infrastructure Report*. Canberra

Commonwealth of Australia. (1979a). *Protective Security Review (unclassified version)*. Canberra: Australian Government Publishing Service.

Commonwealth of Australia. (1979b). *Protective Security Review Report (confidential version)*. Canberra: Australian Government Publishing Service.

Commonwealth of Australia. (2007). Good Security Good Business. Canberra: Attorney-General's Department.

Commonwealth of Australia. (2009). *Cyber Security Strategy*. Canberra: Attorney-General's Department.

Commonwealth of Australia. (2010a). *Critical Infrastructure Resilience Strategy*. Canberra: Attorney General's Department.

Commonwealth of Australia. (2010b). *Critical Infrastructure Resilience Strategy Supplement: An overview of activities to deliver the Strategy*. Canberra: Attorney General's Department.

Commonwealth of Australia. (2011). *Organisational Resilience Position Paper for Critical Infrastructure Australian Case Studies*. Canberra: Attorney-General's Department.

Commonwealth of Australia. (2012a). CERT Australia: Australia's National Computer Emergency Response Team Retrieved 2 November, 2012, from https://www.cert.gov.au/

Commonwealth of Australia. (2012b). *Research Paper 1: CEO Perspectives on Organisational Resilience*. Canberra: Attorney-General's Department.

Council of Australian Governments. (2011). *National Strategy for Disaster Resiliencne: Building the resilience of our nation to disasters*. Canberra: Emergency Management Australia

Department of Homeland Security. (2009). *National Infrastructure Protection Plan: partnering to enhance protection and resiliency*. Washington DC: Department of Homeland Security.

Gibson, C. A., & Tarrant, M. (2010). A 'conceptual models' approach to organisational resilience. *The Australian Journal of Emergency Management, 25*(2), 6.

Kendra, J. M., & Wachtendorf, T. (2003). Elements of resilience after the World Trade Center disaster: reconstituting New York City's Emergency Operations Centre. *Disasters, 27*(1), 37–53. doi: 10.1111/1467-7717.00218

McAslan, A. (2010a). The Concept of Resilience: Understanding its Origins, Meaning and Utility. Adelaide: Torrens Resilience Institute.

McAslan, A. (2010b). Organisational Resilience: Understanding the Concept and its application Adelaide: Torrens Resilience Institute.

Moteff, J., & Parfomak, P. (2004). CRS Report for Congress. Critical Infrastructure and Key Assets: Definition and Identification: Congressional Research Service: Resources, Science and Industry Division.

O'Donnell, K. (2011). *From guns gates and guards: the development of Australia's critical infrastructure protection arrangements, 1978–2010.* Master of Criminology and Criminal Justice (Honours), Griffith University, Brisbane.

O'Donnell, K. (2012). Exploring the development of critical infrastructure protection arrangements in Australia: changing concepts and definitions *Resilient Infrastructure* (Vol. 2 pp. 15–17). Brisbane, Qld: Queensland Department of Transport and Main Roads.

President's Commission on Critical Infrastructure Protection. (1997). *Critical Foundations Protecting America's Infrastructures—The Report of the President's Commission on Critical Infrastructure Protection*. Washington.

Protective Security Coordination Centre. (2002). *Business-Government Taskforce on Critical Infrastructure—The protection of infrastructure from physical attack*. Canberra: Protective Security Coordination Centre.

Ridley, G. (2011). National Security as a Corporate Social Responsibility: Critical Infrastructure Resilience. *Journal of Business Ethics, 103*(1), 111-125.

Rudd, K. (2008). The First National Security Statement to the Parliament. *Prime Minister of Australia, The Hon. Kevin Rudd MP (Archived as at 24 June 2010).* Retrieved from http://pmrudd.archive.dpmc.gov.au/node/5424

Sheldrick, J. A. (1986). The Vital Installations Program. In J. O. Langtry & D. Ball (Eds.), *A vulnerable country? Civil resources in the defence of Australia* (pp. 512-520). Canberra: Australian National University Press.

Tasmanian Government. (1997). Tasmanian Lifelines Project: Hobart Lifelines Project Report July 1997: State Disaster Management Committee.

The White House. (1995, 21 June). US Policy on counterterrorism Retrieved 15 May, 2012, from http://www.fas.org/irp/offdocs/pdd39.htm

The White House. (1996, July 15). Executive Order 13010 of July 15, 1996—Critical Infrastructure Protection. *National Archives Federal Register - Executive Orders* Retrieved 15 May, 2012, from http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=1996_register&docid=fr17jy96-92.pdf

TISN for Critical Infrastructure Resilience. (2004). CIRNEWS for owners and operators of critical infrastructure. *1*(3), 12.

Trusted Information Sharing Network. (n.d.). The TISN. *TISN for Critical Infrastructure Resilience* Retrieved 15 August, 2012, from http://www.tisn.gov.au/Pages/the_tisn.aspx

Trusted Information Sharing Network for Critical Infrastructre Protection. (2010). *Achieving IT Resilience: Summary Report for CIOs and CSOs*. Canberra: Attorney-General's Department.

Yates, A. (2003). Engineering a Safer Australia—Securing Critical Infrastructure and the Built Environment. Canberra: Engineers Australia.

ACKNOWLEDGEMENTS

The author acknowledges Mr Mike Rothery and his team, as well as Professor Mark Finnane, Dr Rebecca Wickes, and Professor Simon Bronitt for their helpful comments on earlier drafts of this paper. Thanks are also extended to the two anonymous reviewers—your suggestions have added much to the paper.

ABOUT THE AUTHOR

Kate O'Donnell holds the degrees of Bachelor of Business, Master of Arts, and Master of Criminology and Criminal Justice (Hons). She is presently a candidate for the degree of Doctor of Philosophy (PhD). Her research currently focuses on the policing of disruptions to critical infrastructure by issue motivated groups (IMG). Before commencing her doctoral studies, Ms O'Donnell was a senior officer in the transport sector of the Queensland State Government who in 2011 was seconded to Center of Excellence in Policing and Research (CEPS) as a Practitioner-in-Residence. In this role Ms O'Donnell worked to include transport security as part of the CEPS research agenda, building strong linkages with the transport sector and undertaking research into Australia's critical infrastructure protection policies. In a career spanning almost thirty years in the Queensland Public Service, Ms O'Donnell has held senior roles in human resource management and industrial relations, health administration, ministerial and parliamentary liaison, as well as transport security.

- o O o -