A Tale of Two Cities: Approaches to Counter-Terrorism and Critical Infrastructure Protection in Washington, DC and Canberra

L. Armistead¹ and J.M. Malone²*

¹ PhD Candidate, Information and Computer Science
Edith Cowan University
Email: leigh.armistead@1984.usna.com

² Chief of Defence Force Fellow
Australian Defence Studies Centre
Email: jeffrey.malone@defence.gov.au

*The views contained in this paper are solely the authors’ own, and should not be construed as representing the views of the Australian government, the Australian Department of Defence, or any other organisation. The paper is unclassified in entirety, and has been cleared for public release.

ABSTRACT

All nations undertake a variety of activities to protect their citizens from the threat posed by terrorism. In the last decade, the requirements of effective counter-terrorism (CT) policy have become more demanding as the result of the changing nature of global terrorism, and the challenges posed by the requirement to protect vulnerable critical national infrastructures (CNI). Since the events of 11 September 2001, of these policies has taken on an unprecedented importance. But the approaches taken by different nations regarding national CT and critical infrastructure protection (CIP) policies have varied considerably. In this paper, the authors will examine the approaches to CT and CIP policies adopted by two nations – the United States and Australia – both before and after 11 September 2001. The paper concludes by proposing explanations for the different approaches in CT and CIP policies adopted by the United States and Australia.

Keywords: Australia, counter-terrorism, critical infrastructure protection, United States

INTRODUCTION

Over the last few years, there has been much written on the potential threat posed by ‘cyber-terrorism’: the targeting of computer networks and related infrastructures by individuals or groups for terrorist purposes. But much of this literature has been sensationalist, has focused narrowly on technical computer security issues, and has failed to link the discussion of ‘cyber-terrorism’ with the broader issues relating to either terrorism or policy responses to it (Lewis 2002; Conway 2003; Devost 2003). Yet it is precisely because of the inter-dependence between the changing nature of global terrorism, and the increasing vulnerability of CNI, that cyber-terrorism becomes a plausible threat (Homer-Dixon 2002). This paper examines the CT and CIP policies of the US and Australia, both before and after 11 September 2001, in light of the changing nature of global terrorism. The paper concludes by offering some explanations for the differences in approaches to CT and CIP policies adopted by each state.

US COUNTER-TERRORISM AND CRITICAL INFRASTRUCTURE PROTECTION POLICIES PRIOR TO 11 SEPTEMBER 2001

During the Cold War, United States national security policy was focused on minimising the possibility of strategic nuclear attack by the Soviet Union. There was a general understanding of the nature of the threat posed by the Soviet Union, and most of the international security efforts of the US (and the West in general) were directed at countering it. But with the collapse of the Soviet Union in 1991 - and with it the
bi-polar world order - the strategic certainty provided by this structured threat disappeared. The spectre of global nuclear war was replaced by a range of diffuse and unstructured threats and challenges (Millett 2003). The reality of the new security environment was brought home to the US with the bombing of the World Trade Center in February 1993. A little over two years later, the scene was replayed when domestic terrorism struck at the nation’s heartland on the morning of 19 April 1995 at the Alfred P. Murrah Federal Building in Oklahoma City.

These events raised awareness of the threat posed by terrorism to the US, but tangible policy outcomes took a little longer to emerge. The first key Clinton Administration response to the evolving terrorist threat was to promulgate Presidential Decision Directive (PDD) 39 – US Policy on Counter-Terrorism, dated 21 June 1995 (Whitehouse 1995). PDD-39 articulated a four-point strategy that sought to reduce vulnerability to terrorist acts, to deter terrorism, to respond to terrorist acts when they occur, and measures to deny terrorists access to weapons of mass destruction (WMD) (ibid.). The four-point strategy integrated both domestic and international measures to combat terrorism. PDD-39 was novel in that it specifically identified the vulnerability of CNI and potential terrorist employment of WMD as issues for concern (ibid.). But in general, PD-39 generally lacked sufficient bureaucratic teeth to achieve meaningful outcomes.

But a clear outcome of PDD-39 was to raise the profile of CIP policy. US policy CIP was not a novelty per se. But previously CIP policy had tended to be overshadowed by other elements of US national security policy (Cordesman & Cordesman 2002: 1-2). And the increasing inter-connectedness of CNI had created a range of dependencies and vulnerabilities that were historically unprecedented (ibid.: 2). PDD-39 directed the Attorney-General to establish a committee to review and report upon the vulnerability of CNI to terrorism (Whitehouse 1995; Vatis 1998). In turn, this committee – the Critical Infrastructure Working Group (CIWG) – noted that CNI was vulnerable not only to attack by physical means, but conceivably also by computer-based means (ibid.). As the result of the lack of knowledge of the cyber threat, the CIWG recommended that a presidential commission be established to more fully investigate this matter.

The CIWG’s recommendation led to the establishment of the Presidential Commission on Critical Infrastructure Protection (PCCIP) on 15 July 1996 by Executive Order (EO) 13010 (Whitehouse 1996). Whilst the PCCIP was primarily a response to PDD-39, in an informal sense it also consolidated a range of uncoordinated CIP policy development activities occurring across government (NCS 1993; IITF 1995; SAIC 1995; DSB 1996; Moynihan 1997; Rattray 2001: 339-340). EO 13010 also directed the establishment of an interim Infrastructure Protection Task Force (IPTF) within the Department of Justice (DOJ), chaired by the Federal Bureau of Investigation (FBI) (Vatis 1998). The purpose of the IPTF was to facilitate coordination of existing CIP efforts whilst the PCCIP undertook its work (ibid.). The IPTF was chaired by the FBI so that it could draw upon the resources of the Computer Investigations and Infrastructure Threat Assessment Center (CITAC), which had been set up there in 1996 (ibid.). In effect, the IPTF represented the first clear effort to establish coordinating arrangements across different government agencies and with the private sector for CIP.

The final report of the PCCIP – Critical Foundations – was released in October 1997 (PCCIP 1997). The key finding of the PCCIP was that whilst there was no immediate overwhelming threat to CNI there was need for action, particularly with respect to NII protection. The PCCIP recommended a national CIP plan; clarification of legal and regulatory issues that might arise out of such a plan; and a greater overall level of public-private cooperation for CIP. From late 1997 to early 1998, the PCCIP report underwent interagency review to determine the Administration’s policy response (Moteff 2003: 4). But in February 1998 concrete outcomes were already beginning to emerge, as the interim IPTF was amalgamated with the CITAC, made permanent and renamed the National Infrastructure Protection Center (NIPC) (Vatis 1998).
The recommendations of the PCCIP were given practical expression on 22 May 1998 with the release of two policy documents: PDD-62 – *Combating Terrorism*, and PDD-63 – *Critical Infrastructure Protection* (Whitehouse 1998a). These two documents were the culmination of the Clinton Administration’s efforts at policy development for CT and CIP. PDD-62 was a direct successor to PDD-39. It provided a more defined structure for CT operations, and presented a focused effort to weave the core competencies of several agencies into a comprehensive program (Whitehouse 1998b). Also in common with PDD-39, PDD-62 sought to integrate the domestic and international elements of US CT policy into a coherent whole.

PDD-62 also established the Office of the National Coordinator for Security, Infrastructure Protection and Counter-Terrorism (ibid.). It was intended that the Office would facilitate inter-agency activities, and in order to achieve this objective it established three senior executive working groups: the CT Security Group, the Critical Infrastructure Coordination Group and the WMD Preparedness Group. Collectively, the purpose of these working groups was to enhance capability for CT response. But the Office did not have the authority to mandate procedures to executive agencies, so its ability to affect change was limited.

PDD-63 was the document that implemented the recommendations of the PCCIP report, as interpreted through the prism of the inter-agency review panel (Whitehouse 1998c). PDD-63 identified twelve sectors of CNI, appointed government lead agencies for each of these sectors, and established coordination mechanisms for the implementation of CIP measures across the public/private divide. In particular, PDD-63 vested principle responsibility for the coordinating activities in the Office of the National Coordinator (which had been set up under PDD-62). PDD-63 also established the high level National Infrastructure Assurance Council (NIAC), to advise the President on enhancing the public/private partnership for CIP. PDD-63 also called for a National Infrastructure Assurance Plan (NAIP), which would mesh together individual sector plans into a national framework. Finally, PDD-63 authorised increased resources for the NIPC, and approved the establishment of sector Information Sharing and Analysis Centers (ISACs) to act as partners to the NIPC.

In the last year of the Clinton Administration, there were some minor changes to CT and CIP policies. Version 1.0 of a *National Plan for Information Systems Protection* was released in January 2000 (Whitehouse 2000). This was the direct result of the call in PDD-63 for a NAIP (Moteff 2003: 19). But reflecting the priority given to cyber security issues by the PCCIP, it primarily addressed NII protection rather than CIP as whole (ibid.). In June 2000, the Terrorism Preparedness Act established the Office of Terrorism Preparedness (OTP) within the Executive Office of the President. It role was to coordinate CT training and response programs across federal agencies and departments. But like the Office of the National Coordinator established by PDD-62, it had to rely on suasion rather than formal authority to achieve its objectives.

When the G.W. Bush Administration came to power in early 2001, there was some consolidation of existing CT and CIP arrangements. The collection of senior CT and CIP groups were consolidated into one Counter-Terrorism and National Preparedness Policy Coordination Committee (PCC) reporting to the National Security Council (NSC) (Moteff 2003: 8). And whilst some debate occurred on future directions for CT and CIP policy, these bore no fruit prior to 11 September 2001 (ibid.). So in practice, during the first nine months of the G.W. Bush Administration, the bulk of the CT and CIP arrangements in place in the US were largely a legacy of the previous Clinton Administration.

Across the period leading up to the 11 September 2001 attacks, the international aspect of the terrorist threat to the US was becoming more evident. Incidents which demonstrated the international character of the terrorist threat included the 1993 WTC bombing, the June 1996 attack on the Khobar Towers complex in Saudi Arabia, plans to attack US airliners in Southeast Asia in 1996, the attacks on US embassies in Kenya and Tanzania, and the attack on the USS Cole in October 2000. In response to these incidents,
both PDD-39 and PDD-62 incorporated measures to combat terrorism abroad. But whilst the international
dimension of the evolving terrorist threat was acknowledged in policy, this was largely overshadowed by
the domestic aspects of US CT and CIP policies.

AUSTRALIAN COUNTER-TERRORISM AND CRITICAL INFRASTRUCTURE PROTECTION
POLICIES PRIOR TO 11 SEPTEMBER 2001

By comparison to the US, the Cold War did not loom as large in Australian national security planning.
Excepting the extreme possibility of Soviet strategic nuclear attack on joint facilities on Australian soil, in
the wake of the Vietnam War Australian security planners largely focused on a variety of lower-level
potential threats to Australia. By the mid 1970s, these came to be centred on the archipelagic region to
Australia’s immediate north. This did not reflect concern that Australia might come into conflict with
states in this region. Rather, it recognised the geo-strategic reality that any military threat to the
Australian continent must come from the north. So this approach to security planning focused on the
capabilities required to mount an attack on Australia, rather than a specific threat from an identified
adversary (Dibb 1992: 1-15). During the same period, Australia had been almost entirely free of
domestic politically motivated violence. So there was little sense of threat to Australia from either internal
or external sources.

Perceptions of the threat to Australia posed by terrorism changed in February 1978, with the detonation of
a bomb outside the Sydney Hilton Hotel at the time of the Commonwealth Heads of Government Meeting
(CHOGM). Whilst in global terms the bombing was minor (three dead and eight injured), the incident
marked an end of innocence for Australia (Malone 1997: 25). In the wake of the incident, the
government commissioned a review of Australia’s protective security arrangements, including response
arrangements for terrorist incidents (Hope 1979). The review made a wide variety of recommendations
regarding Commonwealth/State cooperative arrangements, mechanisms for employing the Australian
Defence Force (ADF) in support of civil authorities, and enhanced capabilities within the ADF and state
police forces for resolving terrorist incidents and responding to incidents involving explosive devices.
The review also noted the need to identify and protect CNI as an integral part of CT policy (ibid.: 99).

The bulk of Justice Hope’s recommendations were accepted by government, and came to be expressed
principally in the form of the Standing Advisory Committee on Commonwealth/State Cooperation for
Protection Against Violence or SAC-PAV (SAC-PAV 1994: i). SAC-PAV was given responsibility for
the National Anti-Terrorist Plan (NATP), and provided the umbrella under which CT policy, capability
development and acquisition, and cooperative and crisis management arrangements might evolve, at both
the Commonwealth and State levels (Malone 1997: 22-38). Paralleling SAC-PAV, the government also
established the Special Inter-Departmental Committee for Protection Against Violence (SIDC-PAV) to
coordinate CT policy issues at the Commonwealth level. In terms of CIP policy, the key response was the
Vital Installations program, which put in place a variety of measures to protect CNI (Sheldrick 1986).
Whilst there were reviews of the SAC-PAV arrangements in 1986, 1992 (Codd 1992) and 1993 (SAC-
PAV 1994), recommendations for changes to these arrangements were minor (ibid: i.). So the CT
mechanisms that were put in place in the early 1980s remained essentially unchanged until late 2001.

But during the 1990s there was some activity on the CIP policy front. In late 1996, the Defence Signals
Directorate (DSD) reported to government on the vulnerability of the Australian NII to a variety of threats
and hazards, and recommended further government action (IDC-PNII 1998: 1). This led to the creation
of an inter-departmental committee (IDC) that was directed to develop policy for NII protection (ibid.).
The National Security Committee of Cabinet (NSCC) considered the IDC report in August 1999. This
culminated in a government announcement of a five-point strategy for NII protection later that month
(Williams 1999). Whilst these outcomes represented a step forward, concerns were expressed that the
pace of government activity was too slow, and the resources devoted to implementing strategy were inadequate (Barker 1999).

In the lead-up to the Sydney 2000 Olympic Games, there was some enhancement of arrangements for intelligence sharing and the procedures for the employment of the ADF (in particular, its Reserve component) in support of CT and security operations (Williams 2002: 6-8). There was also recognition of the evolving nature of the terrorist threat, in the raising of the Joint Incident Response Unit (JIRU) within the ADF for response to terrorist employment of WMD (ibid.: 8-9). Over the same period, there were some changes to the measures in place for CIP (Yates 2003: 39-41). But these initiatives were effectively minor adjustments to existing policies. And whilst Australian CT capabilities were improved during the Sydney 2000 Olympic Games, the bulk of this additional capability was disestablished at the Games’ completion. So these enhancements were essentially tactical reactions to what was perceived as the specific (and temporary) challenge posed by the Olympic Games, rather than a strategic response to the changing nature of global terrorism.

During the period leading up to 11 September 2001, the international dimension of the evolving terrorist threat was becoming more evident to Australia. Investigations in the mid 1990s indicated that the Aum Supreme Truth sect (sponsors of the March 1995 Tokyo subway attack employing sarin gas) had tested the agent on a remote sheep station in Western Australia (Crother et al 2002). And the Sydney 2000 Olympic Games raised the profile of Australia as a potential terrorist target. But overall, the bulk of Australia’s activities to combat terrorism in the international arena at this time consisted of low-key diplomatic activities

**US COUNTER-TERRORISM AND CRITICAL INFRASTRUCTURE PROTECTION POLICIES AFTER 11 SEPTEMBER 2001**

The terrorist attacks on 11 September 2001 led to fundamental changes to the US government’s approach to CT and CIP issues. On 8 October 2001, EO 13228 established the Office of Homeland Security (OHS), to be headed by the Advisor to the President for Homeland Security (Tom Ridge, previously the Governor of New Jersey) (Whitehouse 2001a). The purpose of the OHS was to develop and coordinate a national strategy to protect the US against terrorist attack, in light new threat posed by global terrorism (ibid.). EO 13228 also established a high level Homeland Security Council (HSC), which was responsible for advising the President on all aspects of homeland security (ibid.).

The following day, appointments were made for the National Director for Combating Terrorism (General Wayne Downing) and the Special Advisor to the President for Cyberspace Security (Richard Clarke) (Whitehouse 2001b). Significantly, Downing had previously been the Commander-in-Chief of the US Special Operations Command (USSOCOM), so his appointment reflected a greater prominence for the international (and overtly military) dimension of US CT policy. Clarke’s duties were formally spelt out on 16 October 2001, with the release of EO 13231. EO 13231 established the President’s Critical Infrastructure Protection Board (PCIPB), which was to recommend policies and strategies for the protection of critical information systems. The same EO also established the high level National Infrastructure Advisory Council (NIAC) to provide advice to the President on the same matter (Moteff 2003: 10).

In July 2002, the OHS released the National Strategy for Homeland Security (Whitehouse 2002a). The purpose of the strategy was to integrate all government efforts for the protection of the nation against terrorist attacks of all kinds (Moteff 2003: 11). In effect, the Strategy updated the measures enacted under PDD-63 in light of the post 11 September 2001 environment. The Strategy did not create any new organisations, but assumed that a Department of Homeland Security (DHS) would be established in the near future (ibid.). In September 2002, the PCIPB released for comment the draft National Strategy to
Secure Cyberspace (Whitehouse 2002b). In effect, this document was the proposed successor to the Clinton Administration National Plan for Information Systems Protection. But whilst the issue of the draft plan was welcomed, concerns were expressed that it lacked the regulatory teeth to prompt action by the private sector (Berkowitz & Hahn 2003).

The most obvious consequence of the revised US approach to CT and CIP occurred in November 2002, with the creation of the DHS (Moteff 2003: 11). This consolidated the bulk of US federal government agencies dealing with homeland security (consisting of over 170,000 employees) into one department headed by a cabinet-level official (ibid.). This represented the most fundamental change to US national security arrangements since their inception in 1947. The DHS is comprised of five directorates (Management, Science and Technology, Information Analysis and Infrastructure Protection, Border and Transportation Security, and Emergency Response and Preparedness) (DHS 2003). Significantly, the DHS closely resembled some of the measures that had been proposed by the US Commission on National Security/21st Century (the Hart-Rudman Commission) (USCNS21: 11-20; Moteff 2003: 8-9). But it was only after the events of 11 September 2001 that the political imperative for significant organisational change for CT and CIP emerged.

Further action continued into 2003, with the release of three policy documents: the final version of the National Strategy to Secure Cyberspace (Whitehouse 2003a), the National Strategy for the Physical Protection of Critical Infrastructures and Key Assets (Whitehouse 2003b) and the National Strategy for Combating Terrorism (Whitehouse 2003c). At the same time, EO 13286 abolished the PCIPB and the position of Special Adviser on Cyberspace Security (Whitehouse 2003d; Moteff 2003: 10). The NIAC was retained, but now reported to the President via the DHS. Combined with the departure of key staff associated with cyber-security issues, these measures raised concerns that cyber-security issues were being marginalised in the new arrangements (ibid.: 23-24). But overall, it is as yet still too early to assess how effective the new measures to protect CNI will be.

Overall, arguably the most evident aspect of the new approach to CT policy has been the involvement of the US in substantial military campaigns in Afghanistan and (controversially) Iraq as part of the Global War on Terror (GWOT) (Whitehouse 2003e: 5). But these two military campaigns have tended to overshadow a range of lower-key military and diplomatic activities across the globe (ibid: 17-21). Also, it should be borne in mind that the GWOT does not represent a fundamental departure from the international aspects of CT policy articulated previously in PDD-39 and PDD-62, both of which incorporated a variety of measures to combat terrorism overseas. Rather, the difference between the GWOT and these previous policies is one of emphasis: the changed nature of global terrorism mandated a CT policy with a more evident international dimension.

AUSTRALIAN COUNTER-TERRORISM AND CRITICAL INFRASTRUCTURE PROTECTION POLICIES AFTER 11 SEPTEMBER 2001

Just as the 11 September 2001 attacks had an immediate effect on US CT and CIP arrangements, the same can be said of Australia. Indeed, it must be borne in mind that the Australian Prime Minister was present in Washington on the day of the attack. The imperative for improved CT mechanisms was tragically reinforced a little over a year later by the October 12 bombing in Bali. Whilst the enhancement of Australia’s CT and CIP arrangements was well underway by October 2002, this event provided added impetus for increasing Australia’s capacity to respond to the threat posed by global terrorism, particularly in response to attacks against Australian interests and citizens overseas.

An initial review of Australia’s CT capabilities in October 2001 made four broad recommendations to Cabinet (Cornell 2003: 4). First, the review recommended an immediate increase in resources for operational agencies, which were now faced with increased demands for their services (ibid.). Second, the
review recommended some organisational realignment (though largely within established departmental boundaries) of a number of CT agencies (ibid.). Third, the review recommended some long-term enhancement of detection capabilities (particularly baggage handling in the aviation industry) and response capabilities within the ADF (ibid.). Finally, the review recommended strengthening of Australia’s legal regime for dealing with terrorism (ibid.). By the end of 2002, the Federal government had enacted the bulk of these recommendations.

There were also changes to arrangements for CIP. These included provision of increased resources, a broadened focus on CNI as a whole (rather than concentrating on NII protection) and improved arrangements for public-private cooperation in support of CIP (NCTC 2003a). Significantly, many of the adjustments to Australian CIP arrangements after 11 September 2001 were similar to the measures enacted by PDD-63, as well as the recommendations of the IDC on NII protection dating from 1998. This suggested that whilst the need to improve Australia’s CIP arrangements had been understood for some time, only now did the political imperative for funding them exist. But criticism continued regarding both the pace and level of funding for CIP activities (Lebihan 2003; Riley 2003; Yates 2003: 51-68).

Complementing these reforms (which focused on operational agencies), changes were also made to the high-level coordinating mechanisms for CT. In April 2002, the Commonwealth and States agreed to a modification of the SAC-PAV arrangements (DPMC 2002). Under the new arrangements, now called the National Counter-Terrorism Committee (NCTC), much of the work previously undertaken by SAC-PAV would continue unchanged. But the new arrangements recognised an increased role for the Commonwealth, and broadened the mandate of the NCTC to include the prevention of terrorism and consequence management of WMD incidents (NCTC 2003b: 8-9). It also increased the role of the NCTC with respect to incidents involving CNI (ibid. 7-8).

Around the same time, the SIDC-PAV was split into two new committees: the Commonwealth Counter-Terrorism Committee (CCTC) and the Commonwealth Counter-Terrorism Policy Committee (CCTPC). The CCTC was to focus on coordinating the Commonwealth’s operational response to terrorist incidents. In contrast, the purpose of the CCTPC was to coordinate the development of longer-term CT policy across the Commonwealth, including the international dimensions of CT policy. Capping the enhancement of coordinating mechanisms, the government announced the establishment of a new National Security Division (NSD) within the Department of Prime Minister and Cabinet (DPMC) in May 2003 (Shergold 2003). One of the key tasks of the NSD is to coordinate CT and CIP policies across government (Wright 2003; Rossi 2003), which it will do by providing the support secretariat for the NCTC and the CCTPC (with the PSCC providing the secretariat for the CCTC).

There were also adjustments in policy directed at the international level. In the wake of the 11 September 2001 attacks, the Australian government invoked the ANZUS Treaty (for the first time in the treaty’s history) as the basis for Australia’s involvement in the GWOT (Howard 2001). This action was reflected the recognition that the changed nature of global terrorism necessitated action at the source, wherever this might be: at home, in Australia’s region, or further abroad (ibid.). This was formally articulated as official policy in early 2003 in documents released by the Department of Foreign Affairs and Trade (DFAT) (DFAT 2003: 36-41) and the Department of Defence (DOD) (DOD 2003: 13-14). So one of the key outcomes in Australian CT policy after 11 September 2001 and the Bali bombing was to increase the relative standing of the international dimension of Australia’s CT efforts.

Australia’s highest profile international CT effort was the deployment of elements of the ADF to Afghanistan (Operation SLIPPER) as part of the GWOT. But this tended to overshadow a range of other lower-key activities that were also been taking place. Since late 2001, Australia had been involved in a vigorous campaign to engage its neighbours on both a bilateral and multilateral basis on a range issues relating to combating terrorism. Most notably, this led to the creation of the post of Ambassador for
Counter-Terrorism in March 2003 to provide a focal point for Australia’s diplomatic efforts to counter terrorism (Cornall 2003: 9). The outcomes of these activities have included intelligence-sharing arrangements, mechanisms to counter money-laundering and terrorist financing, and enhancing the skills of regional police and security forces (DFAT 2003: 39). As with the US, these efforts do not represent a fundamental change in Australia’s foreign policy regarding terrorism. Rather, they represent a change in profile and priority that has arisen out of the recognition of the increased threat posed by global terrorism in the contemporary era.

COUNTER-TERRORIST AND CRITICAL INFRASTRUCTURE PROTECTION POLICIES – THE VIEW FROM TWO CITIES

The overall thrust of CT and CIP policy in the US and Australia was essentially similar prior to 11 September 2001. Well prior to then, the governments of both states understood that the nature of the threat posed by terrorism was changing. This was manifest by the concerns about potential terrorist employment of WMD, and the apparent vulnerability of CNI to terrorist acts. In both states, concerns regarding the vulnerability of CNI tended to focus primarily upon the cyber threat to the NII, as far less was known about the contours of this threat than of more traditional terrorist tactics, or even of potential terrorist employment of WMD. And in both states, the focus of operational CT policy tended to be reactive, in that it was focused on responding to terrorist acts rather than shaping the environment that gave birth to terrorism.

Similarities in policy fundamentals continued post 11 September 2001. In the wake of the 11 September 2001 attack, the resources that both states devoted to CT and CIP activities were markedly increased (though not to the same extent). In both countries, CIP policy expanded from a fairly narrow focus on mainly protecting the NII, to one that encompassed all CNI. And in both the US and Australia, where CT policy had previously focused on domestic response, there was a marked increase in the international dimension of CT policy. Most spectacularly, this was manifest in the conduct of major military operations in Afghanistan and (controversially) in Iraq. But in both states, the international aspect of CT policy also involved a range of lower-profile activities to combat terrorism by shaping the environment from which global terrorism sprang.

But despite the similarities in the CT and CIP polices adopted by the US and Australia, there were also notable differences. Whilst these differences preceded the 11 September 2001 attack, they became more pronounced after that date. In effect, these differences resolved into three key themes. First, the pace, priority and relative level of resources devoted to CT and CIP activities in the US has been consistently higher than in Australia. Second, whereas CT and CIP policy activities were clearly and publicly announced in the US, this has not always been the case in Australia. And third, whilst the demands of enhanced CT and CIP policies led to the most significant overhaul of the US national security machinery since its inception, the organisational response in Australia involved little more than tinkering with existing structures.

There would appear to be three inter-related factors that explain these differences. The first of these is the difference in the level of perceived threat and vulnerability between the US and Australia. In the US, the series of terrorist incidents culminating with the 11 September 2001 attack created a sense of insecurity unparalleled since the height of the Cold War. At the same time, a number of executive level exercises and incidents heightened official concerns from the mid 1990s onwards regarding the vulnerability of CNI. By contrast, terrorist incidents in Australia after the 1978 CHOGM bombing (such as they were) attracted comparatively little attention. The attacks on 11 September 2001 and the Bali Bombing, whilst shocking, lacked the visceral impact of a major terrorist incident on Australian soil. And while there was growing official concern over the vulnerability of CNI, this was of a much lower order than in the US. So
the political imperative for substantial CT and CIP policy action in Australia was, and is, significantly less than it is for the US.

The second explanatory factor is the impact of the difference in political culture between the two states on their conduct of national security affairs. In the US political system, there is a strong separation of powers and the conduct of government is relatively open. This means that highly formalised declared policy and organisational actions are essential (and expected) conditions for achieving effective policy outcomes. By contrast, in the Australian political system the executive arm is far more dominant, the conduct of government is significantly less open, and there is a traditional of relative procedural informality. This means that formally articulated policy documents are neither necessarily expected nor required, for policy implementation. So the relative absence of formally announced policies, and the ad-hoc organisational reforms and adjustments undertaken to enhance Australia’s CT and CIP capabilities, reflect the behavioural norms of the Australian political system.

The third explanatory factor is the difference in magnitude of the inter-agency coordination issue between the US and Australia. As a global superpower and large state, the scale, scope and complexity of the inter-agency coordination problem for the US is significantly greater than that for Australia. Accordingly, in the US there was strong support for the creation of the DHS, whereas such a measure was not generally perceived as being necessary in Australia. Rather, the existing inter-agency mechanisms for coordinating CT and CIP activities were regarded by government as essentially still appropriate for the post 11 September 2001 environment.

CONCLUSION

Since the early 1990s, the nature of the threat posed by global terrorism has fundamentally changed. And in response to the changing contours of this threat, states across the globe have adjusted their CT and CIP policies. This paper has surveyed the policy directions followed by the US and Australia. In particular, the paper has noted that in both states that whilst the overall profile of CT and CIP policies increased after 11 September 2001, the level of concern focused specifically on cyber threats declined. But whilst cyber-terrorism is presently not regarded as a credible threat, it does not follow that this will always be the case (Lewis 2002: 11). So if and when a genuine act of cyber-terrorism occurs (either alone or in conjunction with a physical attack), it will be interesting to observe how effective the CT and CIP measures put in place in response to the physical attacks of 11 September 2001, are at coping with this new threat.

ABBREVIATIONS AND ACRONYMS

ANZUS – Australian New Zealand, United States (Treaty)
CHOGM – Commonwealth Heads of Government Meeting (Commonwealth)
CCTC – Commonwealth Counter-Terrorism Committee (Australia)
CCTPC – Commonwealth Counter-Terrorism Policy Committee (Australia)
CIP – critical infrastructure protection
CNI – critical national infrastructure
CT – counter-terrorism
DHS - Department of Homeland Security (US)
DOD - Department of Defence (Australia)
DOJ – Department of Justice (US)
DPMC – Department of Prime Minister and Cabinet (Australia)
DSB – Defense Science Board (US)
DSD – Defence Signals Directorate (Australia)
EO – Executive Order (US)
FBI - Federal Bureau of Investigation (US)
L. Armistead and J.M. Malone

GWOT Global War on Terror
IITF – Information Infrastructure Task Force (US)
JIRU – Joint Incident Response Unit (Australia)
NCS – National Communications System (US)
NCTC – National Counter-Terrorism Committee (Australia)
NIAC – National Infrastructure Assurance Council (US)
NIAP – National Infrastructure Assurance Plan (US)
NII – national information infrastructure
NIPC - National Infrastructure Protection Center (US)
NSC – National Security Council (US)
NSCC – National Security Committee of Cabinet (Australia)
PCC – Policy Coordination Committee (US)
PCCIP - President’s Commission on Critical Infrastructure Protection (US)
PCIPB – President’s Critical Infrastructure Protection Board (US)
PDD – Presidential Decision Directive (US)
PSCC - Protective Security Coordination Centre (Australia)
SAC-PAV - Standing Advisory Committee on Commonwealth/State Cooperation for Protection Against Violence (Australia)
SAIC – Science Applications International Corporation (US)
SIDC-PAV – Special Inter-Departmental Committee for Protection Against Violence (Australia)
USCNS21 – United States Commission on National Security/21st Century (US)
WMD – weapon(s) of mass destruction

REFERENCES


NCTC (2003a) - Critical Infrastructure Protection in Australia, National Counter-Terrorism Committee, Canberra, 25 March.

NCTC (2003b) – National Counter-Terrorism Plan, National Counter-Terrorism Committee, Canberra, June.


---------- (2001b) – *Executive Order 13231 – Critical Infrastructure Protection in the Information Age*, Executive Office of the President, Washington, DC, 16 October.


---------- (2003d) - *Executive Order 13286 – Amendment of Executive Orders, and Other Actions, in Connection with the Transfer of Certain Functions to the Secretary of Homeland Security*, Executive Office of the President, Washington, DC, 28 February.


