SECTION FIVE

RECONSTRUCTING THE RISK

Theorising Risk

> No disaster's a bastard. Most in fact, have many fathers. Somehow they mature by circumstance into menace. There is no single thing that causes this, no one moment that makes it. Each disaster results from a highly individual, dynamic, but inseparable chain of events.[1]

While the indeterminateness in the philosophy of deterrence appears to provide the concept with a robustness and legitimacy in its application, it also provides for a convenience in the assumption that existing controls already effect some measure of preemption. Consequently, this tends to justify the status quo and legitimises current perceptions of the capability of existing counter-measures.[2] Correlating specific events against the successes of deterrence measures is like arguing why an event did not occur and is unlikely to result in an exegesis that would withstand any detailed rigor. Hence, the tendency to dismiss deterrence as a legitimate concept on the basis that it cannot be sampled or calibrated even further justifies the easily accommodated pretence of fiscal constraint, responsible government and a perpetuation of the status quo. The essence of establishing an effective deterrence framework against asymmetric threats, however, is as much about applying limits, as it is in preventing and reducing risk.

---

[1] S. Cookman, *Iceblink: The Tragic Fate of Sir John Franklin's Lost Polar Expedition*, John Wiley and Sons Incorporated, United States, 2000, p 198.

[2] L. Freedman, 'Does Deterrence Have a Future?', *Arms Control of Today*, United States, October 2000, p 1, (accessed 2 December 2000), http://www.armscontrol.org/act/2000_10/detoct00.asp.

Plato and Aristotle theorised that more things might happen in the future than will actually happen.[3] The difficulty in establishing projections in trends and patterns of threat and risk, is that they are intimately tied to the current and historical perspective. The research throughout this thesis, however, has consistently reaffirmed the misinformation and lack of utility, range and veracity throughout the spectrum of current reporting. While attributable to many causes, most importantly are the systemic variations and errors in the reporting of rates and types of incidents, the classification of data and the processes through which information is collected, collated and processed.

The assessment of threat and risk is derived from a mixture of two inseparable elements – objective facts and subjective views, neither however, sufficient in itself due to the dependency on each other. The essence in establishing and defining risk then lies as much in maximising those areas where there is some measure of control or influence over the outcome, while minimising the areas where there is little ability to change outcomes and the linkage between effect and cause is hidden from us.[4] Only the pathologically risk averse make choices based on the consequences without regard to the probability involved, and only the foolhardy make choices based on the probability of an outcome without regard to its consequences.[5] While methodologies for the assessment of risk are intended to reflect a balanced quantitative and qualitative analytical process, forecasting and analysis extends far beyond the possibilities of applying mathematical propositions and weighted indices to projections of non-state activities. *A priori* reasoning cannot eliminate uncertainty from the future.[6] The fundamental issue is then not about assessing risk, but in establishing how to mitigate and minimise those aspects of indeterminateness, and as a consequence, consider those regulatory strategies that when examined in aggregate, may better apply a preemptive capability throughout the national security continuum.

---

[3] Bernstein, op. cit., pp 43-44.

[4] ibid, p 197.

[5] ibid, p 100.

[6] ibid, p 220.

There are no easily dispensed solutions that fill existing voids in international and national counter-proliferation, non-proliferation and anti-terrorism structures. Neither, however, are the current porous and inadequate legislative and regulatory structures contributing any more to the minimisation of risk than the false confidences and expectations of the deterrence capacity of existing measures to influence behavioural change in belligerents. There is no apotropaic set of principles or policy that can easily be adapted or applied to expedite reform. The standard, and now predictable reaction following each crisis is to seek reform through increased punitive measures, more often only exacerbating the problem. The lack of effectiveness throughout many of these ill-considered and reactive measures serves to highlight that there is little room for certainty in the analysis of WMD – only margins of grey and increasingly vacuous areas of uncertainty. The use of deterrence and risk strategies cannot be placed within a context of success or guarantees – only failures. In its idealised form, deterrence theory establishes clear parameters and thresholds, which when crossed, will result in a forceful response, however, the difficulty and complexity in calibrating deterrence measures is in knowing when these lines are approached, or indeed crossed.

This section will examine the further development in the understanding of risk and the propensity towards underestimating the capability of non-state actions, as well as overestimating the capacity by states to influence any outcomes. Previous sections have sought to identify the range of vulnerabilities and limitations encapsulated in the assessment of risk. While this section will look further at those already identified constraints and risks, it will be with the intention of identifying key precepts and strategies and the ability to effect a greater capacity for preemption within the deterrence process.

The methodology applied throughout the section will largely involve an analysis of the varying regulatory contexts and the dependency on the environment in which reform is set, as this is ultimately a major determinant in shaping deterrence measures. An examination of each of the key precepts of detection, reduction, enforcement and response, and the articulation of these into actual deterrence measures and values, is the central theme throughout the section.

There can, however, be no expectation of neatly dispensed and discrete solutions to the problem of micro-proliferation and use. Any reform is premised on an acknowledgement that there is indeed a risk. The complexity of the issue is derived as much from its dependency on accurate recognition, evaluation and actions against threats, as it is from knowing that errors in judgement by states will act cumulatively to increase the success of any corresponding non-state action.

Counter-Strategies and the Non-State Threat

The appreciation of the full range and potential of non-state activities is only a relatively recent phenomen, particularly the ability to understand the evolving lethality and capacity of transnational non-state threats. There still remains, however, a fundamental difficulty in grasping terrorism as a multi-dimensional concept, particularly in all its different social, cultural and religious influences.[7] The preoccupation with purely political aspects of terrorism constrains the definition and further limits analysis outside of often confused and paradigmatic typologies. The context in which any counter-measures are set is equally important in determining their efficacy. The context for these counter-measures is essentially represented throughout three tiered or escalatory levels, represented as active, passive and conciliatory counter-measures. The policies which enact these strategies are applied throughout a range of various interpretative forms by governments. For example, Mubarak's secular Government efforts in Egypt have been primarily directed against increasing Islamic fundamentalism by the Islamic Group (al-Gama'at al-Islamiyya) and Islamic Jihad (al-Jihad). In order to progress the issue of regulatory reform further, it is critical to examine the manifestations of the types of counter-measures and how effective these are as a strategy for deterrence.

---

[7] See B. Hoffman, *'Re-Thinking Terrorism in Light of a War On Terrorism'*, Testimony Before the Subcommittee on Terrorism and Homeland Security House Permanent Select Committee on Intelligence United States House of Representatives, Washington DC, 26 September 2001, and B. Hoffman, *Preparing for the War on Terrorism*, RAND, Washington DC, 19 September 2001.

As with any control process, the permutations and various manifestations will vary considerably, depending on how each state applies measures in response to its own perceptions of the threat. At the core of how counter-measures are to be applied is what is understood in the origins and causes of terrorism. Crenshaw avers that a strategy based on active or repressive measures is in the main predicated on the assumption of an individual and collectivist conception of rationality, with a well established cost-benefit value system already established throughout the non-state structure.[8] These types of counter-measures are in the main effected through the application of repressive measures, most often involving force. Government interventionist policies and actions extend throughout all aspects of arrest, search, seizure, confiscation, and in most cases, such as with the Egyptian and Israeli governments, the denial of many basic human rights.

Turetzky's research on Egypt's active counter-terrorist regime provides one of the more interesting studies on a comparative analysis of the perceived benefits derived from policies which rely on active, ubiquitous and repressive counter-measures. Turetzky argues that contrary to widely held perceptions, such repressive strategies may in fact be counter-productive.[9] Political ostracism, persecution and the deterioration of cultural, social and religious rights, as a result of these types of policies on belligerents and non-belligerents, even further

---

[8] M. Crenshaw, 'The Logic of Terrorism', *Origins of Terrorism: Psychologies, Ideologies, Theologies, States of Mind*, ed W. Reich, Woodrow Wilson Centre Press, New York, 1998, p 9.

[9] Turetzky examines the period of Egypt's repressive anti-terrorism campaign from 1981-1994. Specifically, he attempts to analyse the cost-benefit processes in the Egyptian policy, relying on his own empirical modelling system in attempting to reflect trends. Turetzky's findings suggest that despite the application of disproportionate force against terrorist activity by Muslim extremists, there had surprisingly been a corresponding increase in terrorist activity. That is, the most punitive of counter-terrorism strategies, rather than reflecting an decrease in activity, noted a corresponding increase. Turetzky also superimposes his analytical model over Israel's 'iron fist' policy with a similar result. Turetzky, op. cit., pp 1-24. For a similar analysis of Israel's repressive counter-terrorism strategy, also see F. J. Trapp, *Does A Repressive Counter Terrorist Strategy Reduce Terrorism?: An Empirical Study of Israel's Iron Fist Strategy for the Period 1968 to 1987*, PhD thesis, Florida State University, Florida, 1994.

contribute to the radicalisation and fundamentalism of the disenfranchised.[10] Rather than positively influencing change in the cost-benefit rationalisation of individuals or groups, active policies often resulted in increased levels of terrorist activity. Trends aside, a draconian, repressive and imposing anti-terrorist framework potentially involving purges, expulsions and significant increases in the powers of the security and police organs of government, as Hope identified in 1979, is at a radical disjuncture with the societal fabric of Australia's democratic environment. Such a heightened and active security environment would neither be politically or socially acceptable, nor indeed justified, within the existing threat climate or structure of governance throughout Australia.[11]

Passive and conciliatory counter-measures share some similarities in that both systems are predicated on the attribution of terrorist activity to social, cultural and religious dimensions, rather than its perception as an entirely political entity. A passive approach maintains the capacity to respond punitively by the enactment of various anti-terrorist counter-measures and legislation, yet is more moderated in any approach against belligerents, which is in the main exercised through anti-terrorist controls throughout the criminal legislative structure. Similarly, a conciliatory approach is predicated on identifying the cause of the terrorist actions and then applying interventionist actions which seek to

---

[10] In a more extreme and immediate example of the benefits, or otherwise, of a deliberate and well orchestrated regime of counter-actions by one state against another, an interesting example is provided in the analysis of the United States attack against Libya in 1986. The attack was in retaliation for purported Libyan involvement in the bombing of a Berlin discotheque, which killed two United States nationals. While the air strike had an immediate effect in initially subduing the Libyan sponsored terrorist activity, it ultimately may have been the major contributing factor to a significant escalation of other terrorist activity. The subsequent activities by the Libyans' includes a connection in a plot to bomb a United States military recruiting station in New York on the second anniversary of the air strike; a car bombing, on the same day, of a United States Officers club in Italy and the bombing of Pan Am flight 103 in December 1988. It may also have included the possible involvement of Libyan sponsored terrorists in the bombing of Flight 772, which originated from Chad in 1989. R. M. Boyd and J. J. A. Wallace, 'Deterrence – An Essential Element of Preventing Terrorism', *Australian Defence Force Journal*, Number 116, Canberra, January/February 1996, pp 19-28., and Ilardi, op. cit., p 44.

[11] Interestingly the United States, and possibly the United Kingdom, could both be considered to have imposed forms of active, or indeed in some aspects repressive terrorist counter-measures, although not to the extent of countries such as Egypt and Israel. However, the effectiveness of these regimes has been questioned. There is no empirical data from these countries, at least any of any veracity, that might accurately reflect the effectiveness, or otherwise, in the application of active anti-terrorist measures. For example, increased frequency of arrests and detention may simply reflect increased punitive powers and/or the redefining by states of criminal and antisocial behaviour as terrorist related. For further information by various civil libertarian groups on the relative effectiveness in the implementation of counter-terrorism regimes, particularly for the United Kingdom, see the Statewatch Homepage (accessed 30 June 2001), http://www.statewatch.org. Also see C. Gearty, *Terror*, Faber and Faber, London, 1991.

ameliorate aspects of social, cultural and economic discontent. Countries that maintain extremist anti-terrorist policies would more likely view a conciliatory approach as one that engages the terrorists, and as a consequence, see it as potentially compromising any government. Passive and conciliatory counter-measures, however, remain the only strategies that seek to incorporate both social and technical safeguards, rather than simply relying on greatly increased punitive and repressive measures to enforce any security requirements.

The counter-measures adopted are more often a direct consequence or function of a specific threat or political environment. Increases in religious fundamentalism over the last decade, in particular, have seen counter-measures and strategies aimed specifically at belief, value or psychosocial structures. These measures have attempted to directly influence and constrain activities by attempting to target various terrorist groups, albeit most have been of questionable success.[12] The real danger in any of these systems, however, is the belief that violence and coercion can be delivered in measured, discrete and manipulative doses, dispensed in carefully calibrated increments, to signal this, or that, or to modify behaviour through the exercise of rewards or punishments.[13] At the other end of the spectrum, Australia applies few harmonised or articulated counter-terrorist policies and strategies other than the assumption that counter-measures can be effectively exercised through any existing criminal judicial structure and within the parameters of current national and international laws and normative practices. The strategy is underpinned by the precept that the exercise of the law is based fundamentally on the preservation of life and minimal

---

[12] The study of the dynamics of terrorism can broadly be categorised into two areas: the existence of those with choice and those without. It is this simplistic precept then that in part defines whether there exists the capacity to influence or effect terrorist behaviour, or that measures are then based on the 'inevitability of action' (unlike other arguments that seek to differentiate terrorist behaviour on the basis of rationality). While critical aspects of non-state value systems and organisational dynamics then affect the ability, preparedness and proclivity towards the use of violence (see Section Two of the thesis), the premise that it is causative or a reaction to social, political, cultural or economic circumstances, then establishes the agenda for any policy and mitigation strategies by state parties. For example, this might include attempts to provide remediation measures for minority or oppressed groups. See Crenshaw, op. cit., pp 7-24 and J. M. Post, 'Terrorist Psycho-logic: Terrorist Behaviour as a Product of Psychological Forces', W. Reich, *Origins of Terrorism: Psychologies, Ideologies, Theologies, States of Mind*, Woodrow Wilson Centre Press, United States, 1998, pp 25-40. Also J. Robert, *Psychology and Deterrence*, The John Hopkins University Press, Washington, D.C., 1985.

[13] G. F. Will, *Conservative Chronicle*, United States, 26 May 1993, as cited in A. D. Zimm, 'Deterrence: Basic Theory, Principles and Implications', *Strategic Review*, Volume XXV, Number Two, Spring 1997, p 43.

application of necessary force. While philosophically this is an easy policy to espouse in what appears as a benign or low threat environment, the inadequacy in the structural capability and limited escalatory capacity of national controls, means that the consequences are potentially more profound if this approach is then found to be deficient.

There are various security and policy fora throughout all the national jurisdictions. However, Commonwealth coordination and policy is largely exercised through the Attorney General's Department, most notably through the Standing Advisory Committee on Commonwealth/State Cooperation for Protection Against Violence. There are of course other security fora which draw on a range of departments and services, yet mainly these are predominantly crisis and consequence management structures, such as the Attorney General's organisation, Emergency Management Australia.[14] The vehicle through which national counter-terrorism measures are exercised occurs through the National Anti-Terrorist Plan. The Plan was in the main derived from the outcomes of the 1979 Protective Security Review by Mr Justice Hope. Interestingly, a fundamental strategy established from Hope's Review was the concept of 'lines of defence' – which involved intelligence, preventative actions and crisis management. This is a key concept yet it remains only selectively and inadequately applied throughout the current Australian national security apparatus.

The Special Inter-Departmental Committee for Protection Against Violence was recommended in the 1993 Review of counter-terrorism capabilities as being the responsible agency for the management of national deterrence strategies. Nearly a decade on, however, there remain few measures of any real deterrence value. The focus throughout the committee and coordination structure within the Attorney General's continues as a response orientated and crisis management structure. Even following the 11 September 2001 attacks in the United States,

[14] The structure of Australia's counter-terrorism controls, training and operations draws predominantly on control and coordination being exercised through the Commonwealth Attorney General's Office and the Protective Security Coordination Centre. The Centre is a branch of the Attorney General's and is responsible for administration and coordination support to the wider Commonwealth, States and Territories counter-terrorist committee structure.

reactions by the Australian Government to increase security measures have struggled to move outside of the conventional paradigms of increased barrier controls and wider powers for law enforcement, intelligence, security and immigration services. While there is merit in many of these aspects of increased enforcement, there is little doubt based on initial reporting of these government initiatives, that efforts will continue as ad hoc and lacking in the specificity and definitional criteria that underpins the development of any real efficacy within the controls.[15]

Table 14 – Commonwealth Responsibilities for Counter-Terrorism.

States and Territories have primacy for the enforcement of law and order and there are no mandated responsibilities which define Commonwealth involvement in countering terrorism. Generally however a involvement of the Commonwealth would be limited to:

- Matters of national security concern.
- International relations, agreements and treaties.
- Control of entry/exit of individuals including suspected terrorists.
- Protection of Commonwealth persons/property (including airports, aircraft and passengers).
- Protection of Australian and visiting VIPs and diplomatic or consular staff.
- Protection of Vital National Installations.
- Demands on the Commonwealth (eg release of prisoners held under Commonwealth laws, changes to government policy, statements by Commonwealth ministers).
- Provision of Defence Force Aid to the Civil Power.
- Provision of other Commonwealth resources.

Australia has adopted and implemented a range of limited anti-terrorist legislation, which has in the main been derived directly from wider international norms. Due to the restrictive scope and structure throughout many of the international norms, specifically the lack of capacity to enforce compliance, even in the event of their adoption into national legislation they still remain limited. As a consequence, much of the criminal legislation lacks relevance, capacity and the empowerment to interdict and prosecute use or the escalatory development of specialist technologies and capabilities. Activities involving the development of technical capabilities, such as a CBR WMD (see Appendix Two), relies entirely then on a limited criminal legislative structure to effect any measure of enforcement.[16]

---

[15] There has been little public discussion and consultation regarding the structure and composition of the counter-terrorist initiatives intended by the Australian government in the wake of the 11 September 2001 attacks. The Federal Attorney General, Daryl Williams, released a press statement on 28 September 2001, regarding the intention of the review, stating that it would 'consider the need for consultation' and initially address aspects of immigration, customs, finance and security. V. Burgess, 'Australia's Security to be Beefed Up In the Wake of Terror Attacks', *The Canberra Times*, 25 September 2001.

Not surprisingly, given the structure and application of law and order throughout the different jurisdictions in Australia, the Commonwealth is relatively constrained in its wider counter-terrorist legislative, enforcement and regulatory powers. It predominantly relies on the jurisdictions to apply the micro-regulatory processes that control the proliferation of dual-use capabilities and use. Table 14 identifies those broad areas which define counter-terrorism responsibilities between the Commonwealth and the various jurisdictions.[17] With the exception of response, crisis and consequence management, there are no clear requirements, processes, priorities or policy to effect preemption or deterrence as a national strategy. While it could be averred that wider Commonwealth deterrence responsibilities are exercised through services such as customs, immigration and quarantine, these roles remain relatively disparate and lacking in any harmonisation with other national counter-terrorism requirements, such as targeting, interdiction, suppression and the deterrence of non-state actions.

DEFINING AN AUSTRALIAN RISK ENVIRONMENT

Not surprisingly following the 11 September 2001 terrorist attacks in the United States, there has been wide international opinion in the inevitability of non-state WMD capability development. The general categorisation of the likelihood of an incident as a low threat-high consequence event, however, overly simplifies the spectrum of activities and the potential for use.[18] This thesis has established that while there are technical, engineering and scientific barriers, the capacity to develop a WMD capability can be still be achieved. Albeit, based on current

---

[16] While there are a wide a range of technical regulatory criteria (as noted in Appendix Two), the application and relevance to non-state activities, development or use, ranges between negligible to limited, with controls primarily directed at the regulation of state-sponsored activities.

[17] Personal communication with Mr L. Hansch, Attorney General's Department, 10 September 2001.

[18] For an examination and analysis of the increasing propensity in 'analysis creep' that occurs in predictions of the use of CBR, cyber and WMD capabilities, see P. Chalk, 'Grave New World'. *Forum for Applied Research and Public Policy*, United States, Spring 2000. Washington D.C., pp 13-20.

trends as an indicator, the capability remains some time off.[19] This is not to suggest too sanguine an assessment in either diminishing the requirement for further controls, or that non-state actors are incapable of developing and utilising CBR WMD capabilities – quite the contrary. The introduction of deterrence measures even within a low threat environment potentially provides for increased efficacy in existing controls. As Tour states, 'we should not wait for a national disaster-induced gavel to trigger enhanced controls and safeguards'.[20] The catastrophic 11 September 2001 attacks also further provide a precipitous warning of the need for western democracies to change how they have posited security measures compared to those of the past.

The forthcoming challenge in this lethal and more technically innovative environment will not just be the need to recognise the requirement for wide ranging additional safeguards and deterrence measures, but in ensuring they are effective, consistent and are harmonised with other existing national and transnational threats. In eliciting and maintaining support for greater safeguards and deterrence measures, the difficulty is one of articulating ideals into clearly defined and comprehensive national strategies that apply across the micro and macro regulatory levels of reform. While no regulatory system is impermeable and safeguards can always be circumvented, in the event these technologies or capabilities are used, the more obvious and commonly adopted conclusion is that the structure has failed. The question remains then as to whether a low frequency of incidents or reporting of CBR related activity, reflects the effectiveness of any deterrence strategies, or indeed the contrary.

---

[19] The 11 September 2001 attacks in the United States, which resulted in approximately 3000 fatalities, provides an interesting and complex example of the inherent difficulties in the analysis of WMD capabilities and potential. While no weapons or capabilities were utilised, other than hand held non-explosive weapons to hijack the planes involved, the crashing of a fuel laden passenger aircraft negated the requirement for a bomb or weapon of any kind. While the subtlety of the argument may appear irrelevant, that is, that a WMD outcome can still be achieved utilising simple conventional weapons and that it might negate the requirement for expenditure and analysis on technical unconventional weapons capabilities – it does not. Analysis must still provide for the capacity to anticipate technical, scientific and engineering capability developments and their relative likelihood for use as WMD, even it only as a function of potential.

[20] J. M. Tour, 'Do-It-Yourself Chemical Weapons', *Chemical and Engineering News*, 10 July 2000, p 44.

While frequency of incidents and reporting of activities is used generally to reflect the efficacy of counter-terrorism programs, the reliability and utility of the findings is limited. While there will always be a need to measure the efficacy of any strategies and processes, calibrating deterrence simply on the basis of the organisational capacity to collect and analyse data, demonstrates a proclivity towards misjudgment. In fact, it is this intangible nature within the concept of deterrence that is both its strength and also suggests that it can only ever be effectively calibrated on the basis of potential. For example, trends developing from 2000 in the reporting of the increased illegal activities of the Aum Shinrikyo Cult might possibly only be a reflection of the greater powers of search, seizure and enforcement provided to the Japanese security services from early 1999. While the veracity of the reporting is not in contention, the validity of whether these were enduring or systemic trends, as opposed to simply being caused through a changed security environment, remains an issue of contention and is difficult to prove either way.[21] While the collection of data may assist in providing indications of changing technologies and values, attempting to further calibrate the effectiveness of any deterrence measures simply on the basis of frequency, given the covert and discrete nature of activities, such as micro-proliferation, is to rely on potentially erroneous analysis.

The assessment of the efficacy of any deterrence strategy draws on numerous qualitative indicators. The dynamics and ephemeral nature of terrorism highlight its volatility and the changing environment in which it exists. Indicators must reflect what is being measured. While this appears as obvious, in Turetzky's empirical model, he attempts to calibrate counter-measures on the basis of social, cultural, political and aggregate macro/micro-economic information. Interestingly, he also acknowledges the limitations in these data sets as quantitative calculations of the capability of the regulatory controls and regimes

[21] For an interesting assessment process in the collection and correlation of empirical data reflecting trends in activity (and attribution) of Egyptian and Israeli terrorist activity see Turetzky, op. cit., pp 1-24, and Trapp, op. cit. Both studies attempt to utilise empirical and quantitative analytical models which seek to establish trends in terrorist activities and more specifically, the efficacy of punitive counter-terrorist regimes arguing that repressive policies do not necessarily reflect reduced incidence or a greater effectiveness. Turetzky in particular, however, acknowledges the limitations in the modelling, structure and the veracity of the analysis of trends noting the wide interplay of social and cultural qualitative variables as well simply the uncertainty and indeterminateness of the model.

– which he concludes cannot be accurately assessed through any method – quantitatively or qualitatively.[22]

The calibration of trends based purely on the determination of the threat depends entirely on the level of confidence in the veracity of the processes that detect and reflect signatures of threat (as opposed to variations imposed through other less tangible influences). Ultimately, the non-absolute nature of non-state activities within the current multi-polar international environment makes the application of calibrated levels of deterrence nearly impossible to apply or to measure. Effectiveness, rightly or wrongly, will in the end only ever be defined by perceptions within government and society of the relative safety to the state. It is the factors outside of national and jurisdictional efforts that will more likely shape the threat landscape and while deterrence cannot be viewed as the universal panacea, it will eventually be defined by its ability to influence those factors outside of any immediate effects.

RE-DEFINING CONSIDERATIONS OF RISK

> It is a reasonable assumption that the existence in Australia of police and Australian Defence Force capabilities for countering terrorism, the aviation security arrangements and the system of dignitary protection would figure in international terrorist assessments, although it is not feasible to judge their influence.[23]

Defining and understanding the actual nature of threat and its various elements, particularly when articulated as a national and uniform strategy, is not a new concept, yet consistently this fundamental issue eludes most state parties. One of the most significant findings from the United States Gilmore Commission was the identification of a clear lack of uniformity and consensus in the national

---

[22] Turetzky, op. cit., pp 1-24.

[23] Honan, *Standing Advisory Committee on Commonwealth/State Cooperation for Protection Against Violence 1993 - Review of Counter Terrorism Capabilities in Australia*, p 3.

threat, without which few issues can be progressed beyond mere opinion and speculation.[24] There have been no similar findings *per se* within Australia, yet similarly, and not surprisingly, there remains no uniform strategy, apart from those preparatory and operational measures established within the parameters of the Commonwealth Attorney General's National Anti-Terrorist Plan.[25]

The National Anti-Terrorist Plan primarily addresses prevention, response and investigation processes involving Commonwealth, State and Territory assets. The exclusion, however, of critical aspects of threat and deterrence renders any application of the strategy beyond mechanically prescribed response measures, relatively ineffective in positively influencing any outcomes.[26] While threat analysis and assessment are implicit throughout any coordination and response processes, the range of current measures remains predominantly incident or timeframe specific and reactive to a defined disaster or incident(s).[27] There is no nationally coordinated or uniform threat assessment process which underpins the current range of ad hoc deterrence strategies.

In alluding to the systemic problem in the lack of national coordination and assessment of threat, Hope sought to establish the Australian Security Intelligence Organisation as the primary responsible agency for national threat analysis and assessments. This initiative, however, only fulfilled a small aspect within what should have been a far wider national strategy of deterrence. The dilemma is that intelligence appears as the panacea for deterrence, yet it only contributes a small aspect of any national deterrence capability. Similarly, threat analysis provides an even smaller component of this intelligence function. Despite these inconsistencies, yet which still remain as the drivers to determine how expenditure and resources will be applied, governments still actively expend funds and resources against a problem they cannot even define, and

---

[24] United States Congress, op. cit., pp 9-12.

[25] Honan, *Standing Advisory Committee on Commonwealth/State Cooperation for Protection Against Violence 1993 - Review of Counter Terrorism Capabilities in Australia*, pp 12-13.

[26] Boyd, op. cit., pp 19-28.

[27] Personal communication Mr D. Patterson Emergency Management Australia Australian Department of Defence, 12 April 2001 and Mr P. De Graff, Protective Security Coordination Centre, Commonwealth Attorney General's, 3 April 2001.

similarly, lack the policy and analytical tools against which to calibrate the efficacy of any counter-measures.

The lack of fiscal and equipment priorities is exemplified in current budgetary and resource expenditures by the Commonwealth and jurisdictional governments. Defence and the Commonwealth Attorney General's budgets for CBR capital equipment and counter-measures are in the vicinity of tens of millions of dollars and are still yet to be clearly defined following the 11 September 2001 terrorist attacks. Despite this expenditure, any measures, no matter how well intended, or indeed justified, remain predicated on countering ill-defined and ambiguous estimates of risk.[28] While there is no ambiguity in the function and role of the equipment acquisition projects, or indeed the role of intelligence agencies in their capacity to respond to identified threats, as a national strategy, however, any real role these agencies may have will remain deficient. That is, there is little demonstrated consideration beyond the stockpiling of specialist equipment, the training of first response personnel and the assessment of threat on the basis of simplistic concepts of intent and capability as extrapolations derived from an indeterminate conclusion and a largely preconceived notion of threat.

The Australian White Paper asserts that 'we cannot and should not plan our defence on the basis of any pre-existing threat', yet ironically the existing national deterrence framework is neither commensurate with existing, or indeed any projected, risks.[29] Furthermore, the disproportionate reliance on aspects of

---

[28] Personal communication Mr P. De Graff, Protective Security Coordination Centre, 3 April 2001. Expenditure is approximately four million dollars per year for Commonwealth, State and Territory training expense which includes counter-terrorist training exercises and bomb response equipment. Forty million dollars was expended in 1998 for Defence on 'anti-CBW' equipment and protective gear'. Australian Coalition Government, Defence Policy Statement 1998, *Building Combat Capability*, (accessed 12 July 2000), http://www.liberal.org.au/archive/1998%20election%20policies/defence/defence.html. Additionally, in the Australian Capital Budget Review, the Government has approved a new major capital equipment project (a major capital project is defined as being in excess of AS$20 million) titled Chemical, Biological and Radiological Response Capability (no further information provided). Defence Portfolio Budget Statements 2001-2002, *Capital Budget Overview*, 02 May 2001, (accessed 30 August 2001), http://www.defence.gove.au/budget/01-02pbs/s3_f.htm#CAPITAL EQUIPMENT. There is no data available on expenditure throughout the State and Territory jurisdictions on CBR capabilities, however, most of the equipment and training is utilised as dual-use, that is, it is employed for standard and routine responses for emergencies also involving fire and hazardous materials.

[29] Australian Defence Force Review, *Our Future Defence Force*, Canberra, 2000, (accessed 1 April 2001), http://www.defence.gov.au/consultation2/Dpaper.txt.

response limits any capacity to prevent incidents, rather than just resolving them. This is exacerbated in the limited capacity of the existing structures to deter and counter changed technological capabilities and the *modus operandi* of belligerents, particularly those involved in the use or micro-proliferation of WMD capabilities. In general terms, the CBR WMD threat to date has been limited to low end spectrum use relying more on commercially available precursor chemicals, agents, isotopes, micro-organisms and toxins, normally delivered as acute ingestion hazards (for example food poisonings) or as chronic percutaneous hazards (for example contaminated fragmentation from a detonation/combustion reaction).[30] With the exclusion of the Aum Shinrikyo Cult's release of sarin nerve agent, there have been no significant or effective uses of CBR capabilities which have resulted in multiple fatalities.[31] Current trends of activity reporting (as opposed to reports of interest) reflect markedly different developments, where more often CBR low end spectrum activity appears as unique to single issue groups, geographic regions or a specific threat environment (for example the United States).

It is, however, the aspect of any uncertainty within the threat, particularly at the higher end of the activity spectrum, that exacerbates the influences of two key variables within the assessment process: the greater range and availability of targets and the increasingly transnational and globalised nature of information, communication and travel networks and systems. As Boyd and Wallace conclude, 'no country can expect to be immune from terrorism, even if there are no terrorists or sponsors with a particular grievance against it'.[32] Frustrations in defining activity based on geographical, regional or established associations with other state parties, such as countries that are frequently targeted by non-state actors, further exacerbate and complicate attempts to define and estimate the potential of non-state micro-proliferation and use. While vulnerability is a key aspect in any process involving target selection, conventional or unconventional, it still remains meaningless without wider considerations of threat.

---

[30] Chalk, *Terrorism and Weapons of Mass Destruction Use: An Analysis of Potential Candidate Groups*, pp 17-18.

[31] ibid, p 18.

[32] Boyd and Wallace, op. cit., p 20.

Scientific, Engineering and Technological Developmental Limitations

In defining the scope of the risk, technological, scientific and engineering capacities are an implicit aspect in establishing current and future projections of capability. A critical factor it depends on, and that provides some measure of enduring stability throughout the analysis, is an assessment of the organisational proficiency and technical capacity required to achieve an outcome more significant than simply the release of neat agent or an attempt at crude dissemination.[33] As with capability analysis for conventional weapons systems, technical proficiency and capability are qualitative concepts. Predictive assessments depend on key developmental signatures and identifiers of known activity to establish trends. For example, if reporting indicating unconventional weapon testing against animals was available, it might potentially provide clearer indicators of agent (based on symptoms), dissemination (based on method of delivery) and efficacy (based on results and time over which the testing occurred). Reducing this indeterminateness gap in the understanding of non-state activities, particularly those in relation to aspects of capability development, can be achieved, but will always remain an incomplete process. Effective and specific targeting of collection and sampling resources against key activities in the development process, active and preemptive asynchronous reporting, monitoring and surveillance of defined risk materials and legislative empowerment to act decisively against escalatory development activities, are all key preemptive strategies that not only narrow the gaps in understanding, but also reduce critical aspects of own risk.

While there is no clearly defined or established critical path in CBR non-state capability development, achieving an acute inhalation hazard utilising an effective dissemination system remains the major hurdle for non-state actors. Assessments of capability might normally focus on the acquisition of equipment or chemical precursors, biological seed stock or radioisotopes, however, the greater component within the capability development process lies in increasing

[33] *2000 Monterey WMD Terrorism Chronology.*

the utility of the agents via key capability processes, such as dissemination. Applying counter-measures against capability development processes is complex and related to the provision of unique skills and services rather than simply the regulation of specialist equipment or materials. Counter-measures could include the increased regulation and reporting of particulate, fluid and solid aerosolisation capabilities along with wider reporting structures throughout those areas involving the provision of specialist services. The costs and the risks are increased to the non-state organisation in seeking the necessary materials (through the greater potential for signatures of activity and thereby greater risk of interdiction) by the need to operate in a heightened regulatory and security environment. Essentially the capability and outcome envisaged can vary significantly from that which is practicably achievable and it is this variance that is then 'the aggregate of all the opportunity costs paid in the effort to achieve' what was originally intended.[34]

Organisational Dynamics and Structures

Vulnerability is implicit within any national regulatory structure and while deterrence strategies are directed at reducing the state's exposure to risk, equally it is about imposing organisational risk on the non-state group. While increased regulatory efforts appear to be directed at attempting to alter external aspects in an organisation's behaviour, such as acquisition, internal factors will have a significant heuristic influence in defining the capacity to act, develop or utilise CBR capabilities. The limitation in analysis of the non-state organisational dynamic, however, is in the identification of intent and potential. These factors are entirely predicated on *a posteriori* reasoning due to an information vacuum and difficulties in collection against non-state organisations. Inevitably, it is this paucity of knowledge in understanding non-state organisations that disproportionately dominates and ultimately (mis)defines states' perceptions of their own risk from non-state threats.

---

[34] Zanders, op. cit., p 24.

Zanders argues that the determinant within the organisational structure as to whether the non-state group decides to adopt and use a CBR WMD capability is dependent on its physical and material base. This, however, applies a pragmatism to organisational dynamics that over simplifies what is an abstruse and multi-dimensional issue.[35] The main determinant that establishes the requirement to develop and use a CBR WMD capability is the organisation's value system. While physical and material constraints may influence this, they are limitative rather than causative. That is, what defines the level of capability is not just the weapons available to the non-state organ, but the capacity, values and the preparedness they may have to employ these.

Articulating the identification of specific beliefs or values into an effective strategy of deterrence, is not easily achieved. While increased collection against identified people and organisations is obviously one aspect, the ephemeral and amorphous nature of non-state organisational structures makes even this increasingly difficult. Deterrence strategies and social safeguards that seek to curb organisational developments are long term initiatives. Counter-measures rely on economic and cultural reform rather than more quantifiable measures imposed through increased technical regulatory structures to inhibit violence. Such strategies could include social and amnesty programs for the disaffected, economic reform aimed at reducing support for organisations and educational initiatives to reduce the regional, cultural and religious measures, and specifically, decreasing the political influence many non-state organisations may have throughout their communities of common interest.

Any counter-measures that seek to influence cultural, social and behavioural norms must, however, be exercised and applied with extreme caution and foresight. Initiatives in some circumstances may be perceived as an external threat to the organisation. The consequence may then be that many social reforms, regardless of their more noble intent, may be perceived as a threat, and indeed counter-productive, to the ideal in which they were originally intended. The outcome of these perceived threats may be a potentially reduced internal

---

[35] Zanders, op. cit., pp 26-27.

divisiveness, and consequently, an increased unity and cohesion within the non-state organisation. These counter-productive influences then create a more effective and determined belligerent or organisation.[36]

A National Propensity Towards Risk Taking

The extant structure of regulatory controls within Australia provides an interesting profile in the differences between the actuality of the controls and the perceptions and expectations of any utility.[37] Despite a wide array of seemingly applicable regulatory structures and a perception of a quarantined risk environment from transnational threats, the reality is otherwise.[38] Throughout the spectrum of the regulatory legislation, the capacity to enforce compliance is diminishing in many areas. Processes are increasingly based on self-regulation, discretionary reporting, self-assessment, out-sourcing, devolution of responsibilities and greater competition for resources, with the opportunity cost more often being the reduced efficacy of any security measures. These factors, when further combined with inadequately structured controls, incomplete definitional criteria and an emphasis on pecuniary rather than custodial punitive measures, weakens any realisation of preemption within existing security and regulatory structures. These limitations, when contrasted against the wider global proliferation of WMD technologies and increasing interest by non-state actors in CBR capabilities, suggests there is a real, but not as yet, unrealised risk.[39] If this risk becomes no longer acceptable it will most likely be through the impetus of increased public perception and alarm, international pressure, or

---

[36] A. Bandura, 'Mechanisms of Moral Disengagement', in *Origins of Terrorism: Psychologies, Ideologies, Theologies, States of Mind*, ed W. Reich, Woodrow Wilson Centre Press, Washington, D.C, 1998, pp 165-167. and J. M. Post, 'Terrorist Psycho-Logic: Terrorist Behaviour as a Product of Psychological Forces', in *Origins of Terrorism: Psychologies, Ideologies, Theologies, States of Mind*, ed W. Reich, Woodrow Wilson Centre Press, Washington, D.C., 1998, pp 38-39.

[37] *Sunday Program*, 'Interview Mr P. Reith, Australian Minister for Defence' (video recording), Channel Nine, 30 September 2001.

[38] The perception of the terrorist threat within an Australian environment draws on, *inter alia*, Honan, *Standing Advisory Committee on Commonwealth/State Cooperation for Protection Against Violence 1993 - Review of Counter Terrorism Capabilities in Australia*. The report critically acknowledges (paragraph 108) the problem and divergence between the perception and the actuality of the threat environment. Specifically, it acknowledges 'a slow process in the realisation of the evolution of the threat' and the difficulty in the calibration of the threat, other than through the more general and unreliable reporting the rate or frequency of the incidence of terrorist activity.

[39] Central Intelligence Agency, op. cit., pp 1-12.

more ominously, as a direct result of a national crisis involving the proliferation or actual use of CBR capabilities, rather than simply an identified national security need.

The area of greatest vulnerability for micro-proliferation of CBR capabilities lies in the largely uncontrolled and unregulated area throughout the public domain. That is, those activities generally beyond the point of sale. There remain few effective regulatory processes within this largely vacuous environment other than some related to functions of safety, health and dangerous goods. Even these measures, however, remain only relevant to the specific environment in which they were enacted. For example, these may include a designated workplace or application, such as research or agricultural use.

Trends throughout many of the micro-regulatory structures suggests they are being eroded through aggressive deregulation, decentralisation and by increasing pressures for wider globalisation of trade, research and industry activities. While there are numerous financial benefits throughout many of these wider 'good business' initiatives, they are also major factors in reducing the efficacy of inspection, compliance and enforcement practices throughout regulatory structures. For example, while programs such as the Phytosanitary Agreement within the World Trade Organisation exhort the need for greater standardisation in technical and trade barriers for human, animal and plant standards, participant governments are also obliged to recognise that imported products from other participant countries originate from pest or disease free areas.[40] This is predicated on an assumed comparable, or greater, risk management strategy having been adopted. Regimes such as the Chemical Weapons Convention demonstrate the lack of obligation numerous states have in fulfilling their compliance requirements and the measures they go to in attempting to circumscribe these. The assumption that international normative practices provide any national security certainties, particularly when all lack any

---

[40] D. Gascoin, D. Wilson, C. McRae, *Quarantine Policy in the WTO Environment*, Australian Quarantine and Inspection Service Publication, Canberra, 2000, pp 2-8, and D. Wilson, D. Gascoine, *National Risk Management and the Agreement on the Application of Sanitary and Phytosanitary Measures*, Australian Quarantine and Inspection Service Publication, Canberra, 2000, p 6.

verification capacity or an adequate challenge mechanism, is to premise security on potentially unrealised expectations and false confidences.[41]

A critical aspect of residual risk which permeates most regulatory structures, is that consistently most normative practices lack the necessary compliance mechanisms, either through an ineffective legislative structure, inadequate punitive measures or simply no commensurate enforcement system.[42] Enforcement is generally applied through pecuniary and custodial punitive measures, however, the emphasis on the preservation of human life and individual rights precludes repressive social re-engineering policies (for example, internment without trial and confiscation of land or possessions) and capital punishment. The Commonwealth espouses a philosophy of prevention, containment and defeat in its approach to dealing with non-state actions, yet ironically limits any capacity to apply these measures.

Hope's national review of counter-terrorism in Australia established as sacrosanct the use of the 'same law enforcement framework that applies to any other form of extreme violence, that is, within the existing law by the existing law enforcement bodies [which] will have recourse to military aid only as a last resort'.[43] More precisely, Hope expressed grave concerns that the adoption of strengthened anti-terrorist controls increases the risk that any arrangements could be 'brought into play in dealing with legitimate protest action and public demonstration'. While Australia's same counter-terrorism position, which was premised on those principles Hope identified in his 1979 Review, has been in place for over two decades, it has failed to reflect changing security and safety concerns as well as adapting to a changed threat environment. In essence, what

---

[41] A. Sands, and J. Pate, 'Chemical Weapons Convention Compliance Issues', in *The Chemical Weapons Convention: Implementation Challenges and Solutions*, ed J.B. Tucker, Monterey Institute of International Studies, Washington, D.C., April 2001, pp 17-22. Also see A. Kelle, 'Overview of the Past Four Years', in *The Chemical Weapons Convention: Implementation Challenges and Solutions*, ed J.B. Tucker, Monterey Institute of International Studies, Washington, D.C., April 2001, pp 9-16.

[42] There are of course the obvious provisions within the jurisdictional criminal codes related to conspiracy, homicide and the use of explosives, deleterious or dangerous substances, however, the reference to the lack of enforcement refers specifically to the various applications of therapeutic chemicals, dangerous goods codes, agricultural and veterinary poisons, industrial chemicals and drugs and poisons schedules, within a context of enforcing the regulation of high toxicity/utility CBR materials.

[43] Sands, op. cit., p 19.

has resulted from the exclusion of these principles, is a skewed position in the level and capability of any national preparedness. Specifically, there is a limited capacity to deter, contain or defeat the changed nature of non-state threats.

While the regulation throughout the CBR sectors involving research and trade activities may appear removed from considerations of national counter-terrorism initiatives, it is the ability to act decisively and with a preemptive capacity throughout these sectors that will determine a state's ability to insure its security. Any illegal or covert attempts at development almost certainly will have had its seeds sown within legitimate activity. Germination will have been facilitated through porosity and a systemic inadequacy throughout the system of control. The principles of effecting sound counter-terrorism policy will then be predicated on the ability of discriminatory and targeted regulatory and control practices that act like a tripwire. The ability to capture and assess activities, such as a report of the theft of materials, the procurement of risk agents or the failure to comply with handling, storage or transport criteria, offers the widest, and earliest, capacity to identify signatures of micro-proliferation and development. Yet it also depends on having the technical and social safeguards in place and that the measures are also applied and employed effectively. The national and jurisdictional regulatory environments, at least as they currently exist, retain only a minimal trigger capacity, little to no security value and essentially no preemption within their structure.

Unlike the regulation of chemicals, the biotechnology sector has no established regulatory processes or a statutory body through which to oversee any industry activities, safety or national strategies. With the exception of some areas involving specific processes or technologies, such as those within the Interim Gene Regulators Office, the biotechnology environment exists within a largely

unregulated environment.[44] The inherent risk throughout this sector, which could only be considered as extremely vulnerable, is best exemplified in frustrations by the Australian Bureau of Statistics to even define the scope of national activity throughout the sector. The Bureau has advised that it will be many years before an effective national activity database can be developed like those in the nuclear and chemical sectors, simply due to the difficulties in defining the nature of the industry.[45]

None of the national regulatory environments, however, provides any of the security assurances necessary. There are existing discriminatory regulatory and legislative processes that do offer at least some potential for improvements in reform, particularly those applied to the control of chemicals and radioisotopes. These measures are mainly based on the assessment of hazard (derived from factors such as mammalian toxicity) and are determined by the impact on human, animal and environmental safety, rather than the utility of the materials for misuse or their security. Compared to the biotechnology regulatory structures, the environment in which chemicals are controlled nationally provides many of the necessary regulatory structures and legislative processes. Many of these already incorporate wide reporting, monitoring and verification

---

[44] There are a wide range of regulatory bodies within the biotechnology sector, however, the primacy in the efforts of these bodies appears directed towards new and emerging technologies. An example is the Interim Office of the Gene Technology Regulator and the Genetic Manipulation Advisory Committee, which is responsible for all aspects of gene technology. There are government bodies established to facilitate development and provide advice to industry and government, but there is little mandated regulatory capacity within their functions, such as the non-regulatory body, Biotechnology Australia. There are regulatory bodies associated with disease and quarantine services, similarly however, these are also limited and are generally specific to the application of containment and quarantine controls.

[45] Personal communication Mr D. Byars, Australian Bureau of Statistics, 7 June 2001. One of more recent examples that highlights this increasing risk within this sector involved the release of findings by biotechnology researchers at the Co-operative Research Centre for Biological Control of Pest Animals in Canberra in 2000. The research took a serendipitous turn when in seeking to develop a biological contraceptive for mice, researchers inserted a gene which effected immunity, consequently making the virus deadly to mice. While the mousepox virus does not infect humans, there is concern that the technique could be adopted by state or non-state parties who may have an interest in developing a biological warfare agent. This research is not in breach of the Australian Crimes Act (Biological Toxins) 1976 or the Biological Weapons Convention. The work was carried out by academic researchers, not by government or contractors linked to government research or biological defence programs. Nevertheless, it highlights the potential and vulnerability for exploitation, along with the clear lack of regulatory controls that might stop or inhibit similar research or access to similar types of technologies. E. Harris, 'Research Not to Be Hidden', *New York Times*. New York, 6 September 2001 and M. Frederickson, 'Scientists Engineer Deadly Virus', *Bio Online*, 31 August 2001, (accessed 4 September 2001), http://www.virusys .com/News/Deadly_Virus/deadly_virus.html.

processes, such as those included within the Chemical Weapons (Prohibition) Act 1994.

The national biotechnology sector, in particular, lacks any potential for superimposition of additional regulatory requirements and the strengthening of security functions covering legal, illegal or covert misuse. As a consequence of the considerable requirements for change throughout the sector, reform would only be achieved through the introduction of a complete new range of regulatory legislation. Even current processes which regulate pathogens and infectious materials are simply exercised through one class of dangerous goods. Comparatively, the regulation of chemicals is exercised across eight different classes of chemicals classified on the basis of physical characteristics and risk. Diagram 5 is representative of this wide disparity in regulation and enforcement across the different CBR sectors.

DIAGRAM 5 – THE NATIONAL REGULATORY AND ENFORCEMENT SYSTEM

BIOTECHNOLOGY SECTOR	CHEMICAL SECTOR	RADIOISOTOPE SECTOR

INCREASING REGULATION

DECREASING ENFORCEMENT

In attempting to identify those core determinants that shape and define risk throughout the regulatory processes, the ability to control dual-use services and knowledge remains one of the most significant vulnerabilities and given its indeterminate nature, a residual and enduring aspect of risk. As already identified in the use and development of the genetically modified mousepox virus by Australian National University Researchers in Australia, the materials and dual-use equipment required for development are more often available commercially. It is the provision of specialist skills, however, that determines whether the capability will have any realised utility, such as those skills involved in chemical engineering processing, hazard modelling and fluid mechanics. The

difficulty is that there are few safeguards, particularly when most of the relevant dual-use service industries are fostered throughout the industry, research and commercial sectors, as opposed to being retained throughout classified military and restricted government sectors and programs.[46]

The provision and supply of dual-use services has two different aspects to it, one active, and the other passive. Passive are those measures referred to in the previous paragraph that involve the increasing availability of dual-use knowledge throughout industry and the public sector, whereas active refers to those aspects involving proliferators actively exploiting service supply and availability opportunities. Active services are best highlighted in the exposure to risk from foreign nationals residing and working throughout Australia as students and researchers. This is a potentially significant vulnerability and remains largely unrecognised and undetectable. Attempts to establish the actual nature of the threat and levels of exploitation activity by these groups will remain a frustrating and indeterminate exercise due to the lack of activity signatures and the dependence on foreign currency by Australian research and academic institutions. While some of this risk can be offset through increased profiling, greater discriminatory vetting and enhanced compliance requirements in visa control processes, it will always be difficult to calibrate any threat accurately. Without clear identification and a wider legislative mandate to correlate and regulate entry against these uncertainties, the residual elements of risk implicit throughout these activities will remain significant, indeterminate and constant.

It is this lack of capacity throughout the national security structure to detect, reduce, enforce and respond to these types of proliferant activities, that cumulatively influences Australia's exposure to risk. Monitoring and surveillance resources and activities appear out of step with established

---

[46] Australia's efforts specifically in the field of research for chemical and biological warfare agent use are limited to defensive research in support of the Australian Defence Force. The research is conducted at the Defence Science and Technologies Organisation in the Combat Protection and Nutrition Branch in Melbourne. This is a declared capability and facility under Article X of the Chemical Weapons Convention requirements and is maintained for protective research purposes only. Personal communication with Dr G. Shaw Australian Safeguards and Non-Proliferation Office, Department of Foreign Affairs and Trade, 15 May 2001. Also see Commonwealth of Australia, Initial Declaration, Parts 1 and 2.

information and reporting of the methods of proliferation activity associated with active state WMD programs. For example, Iraq's aggressive and covert attempts to obtain dual-use materials, equipment and services to support state attempts to develop their WMD program highlighted the porosity throughout many states proliferation controls, including Australia's.[47] The case study on the micro-proliferation activities of the Aum Shinrikyo Cult in Section Two of the thesis highlighted the covert, undetectable and often indistinguishable nature of many proliferation activities. This is often further exacerbated in the case of non-state activity when compared to state programs as it will more likely involve reduced quantities of materials or equipment. The unlikely recognition or attribution of much of this activity, simply due to the low volumes and the thresholds involved, which are also often outside normal detection and notification triggers for many non-proliferation regimes, suggests that most activity will continue to be conducted under the pretence of legitimacy and under the guise of legal micro-proliferation.

There are two fundamental considerations which shape current national misperceptions of threat and risk. The first draws from the pretence by government and industry that continues to perpetuate the expectation that there is no real threat, at least any which Australia should be concerned with. The second is the lack of an identified impetus or requirement for change in the status quo, either from external or internal factors. While the second consideration may seemingly appear dependent on the first, the terrorist attacks on 11 September 2001 already counter the first, yet there continues to be little recognition in government or industry for change in the second. The misperception of current capacities and misleading expectations in the effectiveness of extant controls is symptomatic of not just a false confidence and a lack of understanding, but also the simple fact that national security measures have never been validated. This cumulative error limits the capacity to accurately assess and calibrate risk, greatly increasing Australia's overall vulnerability. This failure in the consideration of deterrence as a multidimensional concept resonates throughout all national counter-measures

---

[47] Office of the Secretary of Defence, *Proliferation: Threat and Response*, pp 38-42.

with the result being not only a disproportionate emphasis on response and crisis management, but a lack of any capacity for preemption.

DEVELOPING A NATIONAL DETERRENCE STRATEGY: RISK AVERSION VERSUS RISK TAKING

To focus counter-measures at the accumulation of response capabilities in the analysis of CBR and WMD threats is convenient and provides a pretence of deductive reasoning. The gravitation by governments towards new and more capable detection and analysis technologies and the training of response elements, provides immediate, quantifiable and measurable results for even a modest investment of resources. At its essence is an attempt to circumscribe the threat and suppress, or indeed attempt to overwhelm, the responding asymmetric capabilities – but to what effect? This is not to deny the requirement for effective crisis and consequent management capabilities. A clearly articulated response capacity underlies any capable crisis and consequent management framework, yet the contention remains not in the requirement, but in the balance.

The Australian Attorney General's Department has consistently identified the imbalance in national counter-measures, specifically highlighting the inability throughout the current range of counter-measures to cause any real measure of preemption. As early as 1979, from Hope's review of counter-terrorism capabilities in Australia, and again in the last review in 1993, identified the need for preemption and an enhanced deterrence framework to underpin Australia's counter-terrorist strategy, which continues to be lacking. Specifically, the reviews concluded that there was insufficient focus on prevention within the machinery for strategic oversight of Australia's overall counter-terrorism capability.[48] Yet while there has been a range of counter-terrorism initiatives, reviews, training and policy implemented, from developments in the National Anti-Terrorist Plan to increasing training and exercise regimes, preemptive deterrence measures as part of a wider strategy have been largely reduced to exhortations of the need for strengthened and more intelligence assets. While

---

[48] Honan, *Standing Advisory Committee on Commonwealth/State Cooperation for Protection Against Violence 1993 - Review of Counter Terrorism Capabilities in Australia*, pp iv-v.

there is clearly a benefit in the requirement for more detailed technical intelligence collection, analysis and assessment, this still falls short of harmonising and enhancing existing controls, developing new regulatory regimes and energising processes to more effectively collect, target and interdict non-state capabilities.

Ultimately the question remains as to what deterrence measures can then be adopted as preemptive strategies outside of any counter-measures already in force, and yet that are predicated on the extant judicial structures and still workable. The issue of deterrence is also often dismissed as irrelevant or too qualitative, due mainly to the frustrations in defining and measuring outcomes – particularly within a resource constrained environment.[49] To accept such arguments, however, is to fail to understand the nature of the problem and in doing so, to resign efforts to a passive approach and provide for an immutability and fatalism in any attempts to countering-terrorism. This phenomena is not unlike what psychologists refer to as 'learned helplessness', which describes a perspective of 'disempowerment' in any capacity to act proactively or decisively against developing risks.[50] While not so much a conscious or deliberate action, states may hide behind a veil of self-styled, yet ineffective initiatives, that when an incident does occur, are passed off or attributed to its difficulty, complexity or even simply as bad luck.

While it is well to exercise concerns through the vague policy axioms of minimum force and the preservation of life, articulating these principles into

---

[49] Personal correspondence with Mr L. Hansch, Attorney General's Department, 10 September 2001. Comments made in relation to view maintained by a senior (unnamed) Australia Defence Bureaucrat.

[50] Learned helplessness can be attributable to a series of disabling and unpleasant experiences. In the case of state actions, or inaction, this may be as a result of an incremental series of shocks that degrade the collective sense of the ability to control events. Individually and collectively, behaviour changes to where it is in the main derived from vicarious experiences of what is seen to be happening in the surrounding environment. In this sense, as Argyris aptly identifies, learned helplessness defines a set of behaviours he calls 'organisational defensive routines'. C. Argyris, *Knowledge of Action*, Jossey Bass Publishers, San Francisco, 1993. The apparent inability of states, particularly the United States and Israel, in attempting to stem more deadly and deliberately orchestrated acts of transnational terrorism, often culminating in graphic and catastrophic attacks, cannot but influence the collective psyche of states and their actions. While the lack of deterrence through most counter-measures and the need to focus responses on only aspects of vulnerability and response-centric efforts may be attributable to paradigmatic analysis, it is also likely stems from a collective and individual culture of learned helplessness. J. Warn, 'Overcoming Learned Helplessness', *Australian Defence Force Journal*, Number 150, Canberra, September/October 2001, pp 57-61.

improved policies and regulatory practices, is more complex and difficult. Increasing punitive measures and strengthening the regulation of materials is also about understanding the probable mechanisms of cause and effect which are intertwined throughout the various deterrence structures. As a consequence, if deterrence is to be applied, it must be ubiquitous and permeate all aspects of national activity. The corollary to this is in Hope's unrealistic expectation that if deterrence measures are to be effective, they must be beyond the capabilities of terrorists to evade or otherwise defeat.[51] While a sound theory, the precept fails to adequately incorporate those capabilities that while falling short of the ideal standard will still retain significant deterrence value. As critically, any deterrence measures must be realistic in cost and have regard to resources, yet if further measures become critical to national security, then additional resources must be found.[52]

REDUCTION: A STRATEGY FOR DETERRENCE

Reducing the Risk – The Regulatory Environment

> It is self evident that the ability to anticipate precisely where, when and how terrorists will strike would enormously advance counter-terrorist efforts. That obvious truth gives emphasis to the importance of intelligence. Unfortunately the intelligence coup will almost invariably be less signal.[53]

The application of any deterrence measures by states has normally relied on increases in barrier and exclusion controls, the application of more extreme punitive measures or protestations in the capacity and need for greater intelligence capabilities. Wallace and Boyd define these types of counter-measures on the basis of offensive and defensive strategies. This tends to overly simplify what is actually a complex myriad and interplay of social, political,

---

[51] Hope, op. cit., pp 87-88.

[52] ibid, pp 87-99.

[53] ibid, p 34.

economic and global influences.[54] In particular, there is a need to examine strategies in aggregate where both the technical and social dimensions are included. Whatever the capacity adopted to regulate dual-use materials and equipment, all measures will eventually be capable of being circumvented by the determined belligerent. While this does not suggest technical regulatory measures are not necessary, it does indicate that in aiming to reduce the potential of non-state organisations to act, their reasons and motivations are equally critical in determining how counter-measures and deterrence strategies are to be applied. The same applies to the adoption of social safeguards, that is, without commensurate technical counter-measures that work to provide strong disincentives to acquire, develop or use WMD technologies, any benefit that might otherwise have been derived from these is greatly reduced.

Despite the limited efficacy of, and ability to apply international law in the control of non-state activities, the first step in any deterrence strategy must always be positive, progressive and continuing involvement in international non-proliferation and anti-terrorist norms that actively engage other state parties in establishing more improved normative practices. Australian foreign policy must as a minimum reflect widely established international norms, such as the Convention on the Suppression of Terrorist Bombings. This includes ensuring the full intent and capacity of the norms is reflected throughout national legislation (whether required or not). The greater challenge lies in then attempting to ensure non-state capabilities are covered just as equally as state parties by those normative practices that attempt to control WMD technologies. While the regulation of export controls will always remain at the core of non-proliferation initiatives, the failure to further capitalise on the opportunities inherent within international norms will always see state parties struggling to effect adequate non-proliferation and counter-proliferation strategies.

---

[54] Boyd and Wallace refer to offensive deterrence as the application of repressive strategies and counter-measures involving trade sanctions and refusal to accept the grievances of the non-state actors. Defensive deterrence refers to those policies widely employed to maximise potential costs and minimise possible gains (which in effect is the same aim of many of the offensive deterrence strategies). The division is somewhat confused and difficult to distinguish when placed in a context of foreign policy initiatives, anti-terrorist international norms and social safeguards. Boyd and Wallace, op. cit., pp 23-24.

In essence, international norms will never realise their full potential until they establish clear and uniform mandatory measures for the criminalisation of non-state activities. This also highlights the requirement for state parties' national legislation to have a greater international transparency and increased mandatory reporting and information exchange process. This is not necessarily to suggest the requirement for mandatory reporting beyond national boundaries, which would result in regimes never progressing beyond theoretical social and arms control regulatory models. Rather, it is a requirement to ensure states maintain a capacity and structure, similar at least to the example provided by the Chemical Weapons Convention. This requirement within the Convention, applied through the Office of the Prohibition of Chemical Warfare in the Hague, attempts to ensure standardised compliance and annual reporting processes throughout all participant states.

The internationalisation of national reporting should attempt to establish an obligation on states to ensure increased compliance, not just though export and barrier controls, but throughout all exclusion and protection activities for designated dual-use materials, equipment and services. There already exists significant capacity throughout many regulatory regimes, but these remain unrealised in most cases, such as those throughout the requirements of the Australia Group, Chemical Weapons Convention and Wassenaar Agreement (these regimes are examined in detail in Appendix One). Consistently these international norms lack both the imperative to compel change and the national compliance vehicle in which to enforce measures. While Australia should seek full involvement and the highest degree of international co-operation in establishing measures to counter non-state activity, it must be always be remembered that only Australia can be relied upon to put Australian considerations first. It is therefore critical that throughout all national considerations that depend on the expectations in the capacity of international norms and information sharing arrangements for their capability, that governments remain appreciative and cognisant of the limitations in these structures. In the end, the imposition and enforcement of any regulatory measures will always fall wholly on Australian agencies to adopt, apply or enforce.

Reducing the Risk – Information and Processing Management

For any regulatory structure to provide the necessary discriminatory triggers, it must maintain a capacity to collect information as widely as possible. Frustrations imposed throughout the international security environment in the capabilities of police, customs, immigration, quarantine and intelligence agencies to collect, recognise, process and analyse specialised information, impose significant information processing, resource and personnel costs in the ability to achieve this.[55] Even with successful information collection, the capacity to discriminate critical byte sized packets of technical information from the increasing volumes of background clutter is impossible without calibrated technical, discriminatory and analytical capabilities, which require the resources and the analysts to assess the information.[56] The inability to process information, despite wide collection networks, is best illustrated in an example derived from World War II. The British could read German codes and controlled German spy networks in Britain, yet were in desperate military shape by 1942. The capacity to exploit information makes information dominance more crucial than ever before.[57] Exhortations of greater capabilities must as a

---

[55] United Nations Security Council Resolution 1373 SC/7158 dated 28 September 2001, (which is yet to be adopted as at October 2001), calls on countries to implement a range of measures against terrorist activities. Interestingly, and unlike any other previous resolutions, it seeks to have state parties 'exchange information and cooperate to prevent and suppress terrorist acts'. While the Resolution acknowledges a range of activities, the intent is primarily to establish clear national requirements for state parties in vetting, profiling and in ensuring all available measures are enacted to check people entering or existing national boundaries, prior to the grant of entry or refugee status. It specifically requests that states ensure that asylum seekers have not participated in planning, facilitated or participated in the commission of terrorist acts. This provides not only a clear mandate, but also provides a legitimate justification for the adoption of increased security measures within Australia in attempting to ensure tougher profiling and vetting standards are applied throughout all barrier and exclusion controls, including immigration, customs and quarantine.

[56] The requirement for agencies, from the police through to intelligence services, to ensure they maintain effective and credible analytical capabilities has been an enduring theme throughout the major reviews of counter-terrorism in Australia. Hope was the first to identify the requirement for a technical analytical capability and Honan's later 1993 review reaffirmed a similar requirement, going further in identifying the need to maintain specialist capabilities for analysis of financing, equipping and exercising these capabilities. Hope, op. cit., Section Four, and Honan, *Standing Advisory Committee on Commonwealth/State Cooperation for Protection Against Violence 1993 - Review of Counter Terrorism Capabilities in Australia.*, pp 29-31.

[57] P. Morgan, 'The Impact of the Revolution in Military Affairs', in *Preventing The Use of Weapons of Mass Destruction*, ed E. Herring, Frank Cass Publishers, London, 2000, p 140.

consequence reflect commensurate increases in the capacity to process and analyse information, rather than simply developing as an exercise in collection.

In terms of the mechanics of reduction measures that are nationally focussed, one of the more significant is to be found in the maintenance of strengthened barrier and exclusion controls. These provide the first line of defence and while the predominance of effort will always be directed at the actual geographic barriers involving processing, profiling and vetting at entry and exit nodes, the introduction of deterrence strategies should not be limited to activities at points of entry or those just within continental Australia. For example, education and warning notifications should be included in all foreign nationals' travel documentation at points of embarkation or disembarkation into Australia.[58] The development and application of greater discriminatory profiling analysis has the potential to significantly contribute towards reducing the risk from illegal entry into Australia of non-state actors. Efforts, however, must reflect a significantly enhanced and greater discretionary capacity in the targeting of both people and specified technologies, than is currently exercised.

While there are a number of extant customs, quarantine and immigration profiling systems that already provide for a wide range of discriminatory processes, these remain limited by their origin, veracity and the lack of depth throughout the information used to populate them. Current profiling databases employed by Customs and Immigration in particular, are restricted in their interoperability with other national and international watchlists, relying for triggers of activity based on declared, matched or known information. These systems, similar to the health notification and warning structures, are predominantly shaped as passive detection processes, which depend on the information provided rather than through information actively gained.[59] While the more obvious step of increasing the interoperability of these systems with other criminal and intelligence databases is the first step, there are a wider range

---

[58] Security Council Resolution 1373 seeks to obligate state parties acceding to the Resolution to establish clear preemptive strategies aimed at detection of forged or falsified documents, greater capacities to vet persons entering countries and increased security of activities nationally. SC/7158, op. cit., pp 2-3.

[59] Personal communication Mr Tony Pollock, Director Intelligence Analysis Branch, Department of Immigration, 26 June 2001.

of measures that can result in more immediate and increased security. Most notably, is an enhanced preemptive profiling system for people and cargo along with the greater capacity for integration throughout all the different agency and international alert and watchlists. This also includes an increased capacity for link analysis and cross-matching throughout the different databases to enhance targeting and profiling at national barrier entry and egress points.[60] The current measures, which in the main rely on clearance by exception rather than as a standardised or routine process, carry an unacceptable level of indeterminate risk. Unlike, the risk associated with the regulatory control of materials and equipment, however, the residual risk with barrier and exclusion measures tends to be cumulative. This is particularly so when further considered against other illegitimate and undetectable entry measures and the overall effectiveness, or lack thereof, throughout the range of other national measures used to control and detect people and cargo.[61]

Reducing the Risk – Establishing the Regulatory Context

The environment and context in which regulation is established is as crucial to the efficacy of the regulatory process as is the structure through which it is applied. The volume and diffusion of certain types of activity, along with the difficulty in regulating specific classes of materials and services, suggests that

---

[60] The lack of functionality and interoperability was highlighted in the inability of barrier controls, throughout a range of countries, to recognise, identify and interdict the terrorists involved in the 11 September attacks against the United States. In fact, three of the nineteen were already on FBI alert lists, however, similarly to Australia, the coordination of immigration with customs, police and intelligence agencies relies on liaison rather than the increased functionality that might otherwise be derived from shared information and processes.

[61] The capacity to establish known associations with or participation in, various activities or organisations involved with extremist and/or fundamentalist belief systems is a complex and difficult task and crosses a range of responsibilities for policing, security, intelligence and critically, civil liberties. The fundamental issue, however, is one of greater interaction and a more proactive capacity within the application, exchange and the population of databases, thereby ensuring a more pervasive discriminatory structure to any controls. Existing national levels of interaction with customs, immigration, police, security and intelligence information services, is inhibited through classification restrictions, availability, training, accreditation, and issues of privacy, both as a function of the input of information in the database and the security implications for the release of information outside of its immediate application. The reality is that while this function is constrained, the capacity of barrier controls will remain limited to visual identification of irregularities (via X-ray or observation), notification of known persons and detection of explosives (by explosive detection dog or explosive vapour detectors). Hence, the capacity to circumvent barrier controls through the use of false and/or misleading information (or other means) and the ability of existing vetting and profiling systems, are only of actual benefit if the person obliges Australian authorities by using a known or established identity (and then only if it is actually entered in the Immigration alert system).

large sectors of industry and government will nearly always remain outside of tightly prescribed and mandated regulatory environments. The inability, or lack of need for more stringent regulatory measures, may simply be due to a reduced level of relative risk and/or that it is impracticable to apply controls throughout a complete production or distribution process. As a consequence, it is most likely that the regulation of many lower risk materials in particular, will only ever be sustainable within an environment that relies on self-regulation or self-assessment.

While self-regulatory or assessment regimes are less than ideal for many high risk materials, if regulation is to be adequately enacted throughout the regulatory continuum it may only ever be achievable through the adoption of industry based standards and accreditation criteria, rather than through a mandated legislative environment. An example of this is to be found in the difficulty in establishing rigid end-use criteria throughout the agricultural and mining industries for many cyanides and its derivatives or analogues. Determining end-use in some cases is difficult due to the excessively large volumes and scale of use, making it nearly impossible to adequately account for due to varying consumption, wastage, loss, evaporation and dilution rates.[62] End-use will not always be achievable, yet it can be offset with strengthened risk management practices. Measures may include increased security requirements for specified materials, industries or even certain handling requirements.

Despite the limitations in determining and applying end-use processes, with effective management, reporting and an efficient processing capacity, there still exists the potential to regulate and manage the full spectrum of risk materials that might otherwise never be visible to national and regional security monitoring processes. Most particularly, the potential offered through product stewardship

---

[62] Applying end-use criteria throughout the range of most CBR agents would be limited based on cost or simply through the impracticality in defining a process of any practicality or veracity. End-use is complex and even defining where a cycle completes itself is difficult. Is end-use finalised at the point of disposal, when a product is consumed or when there are changes in its physical state (to include toxicity)? Similarly, does end-use extend to propagation, culturing, gene manipulation or any of the newer genetic engineering technologies, including processes involving the extraction of genetic signatures or markers, such as DNA, from a micro-organisms? There is no standardised answer and each requirement for end-use would need to be determined on the basis of the risk, the materials involved, security and, importantly, considerations of potential.

programs, such as those used by the Plastics and Chemical Institute of Australia, offers significant benefits in the wider control of risk capabilities. Specifically, this includes the Responsible Care Initiative which is currently applied throughout the chemical industry.[63] It defines national and global standardisation measures and attempts to apply regulation and compliance protocols throughout all production, distribution and sales activities.

As a program, the Responsible Care Initiative is one of the more active and preemptive self-regulatory structures applied throughout any Australian industry. While not specifically security focussed, it does, however, attempt to impose responsible handling, distribution and sales standards which consider issues that may impact on product control issues. The initiative obligates participant companies to comply with industry-wide agreements or risk loss of accreditation and exclusion from the industry-wide benefit programs. While this has yet to be applied or enforced against an Australian company or industry group, it does not also necessarily reflect total compliance. Most self-assessment programs, however, only remain viable through voluntary, conciliatory and participative practices, hence, this very issue is at the core of the limitations in the utility of these programs.

There remain many problems with any voluntary program, not the least of which is ensuring full industry participation and the fact that most decisions are nearly always commercially or financially driven. The potential for these types of self-regulatory structures, particularly throughout environments such as the developing biotechnology sector and also for many low risk materials, is that they offer significant potential in areas that might otherwise remain largely unregulated. These programs also serve as a benefit to the industries in terms of the potential for increased efficiencies, greater regulatory standards and the likelihood for the wider control of materials that might otherwise only have been achieved through a legislative mandate. The problem still remaining throughout the process of self-assessment and self-regulation is in the end the reduced capacity for enforcement and the lack of any coordinating or management

[63] Personal communication with Dr M. Mathews, Director Business Development, Plastics and Chemical Institute of Australia, 9 May 2001 and 25 May 2001.

authority, that is, the capacity for an authority to be more than just titular in its role.

Reducing the Risk – Controlling Services and Information

The regulation of information and services remains one of the outstanding and most complex issues to develop and apply deterrence measures or standards against. The wide availability of information throughout a range of mediums means being able to calibrate risk is an uncertain and indeterminate process. In terms of regulating information in published formats, this is the responsibility of the Office of Film and Literature Classification, yet the latitude to regulate literature other than violent or sexually explicit material, is for most parts, extremely limited.[64] The regulation of services is even more difficult to regulate and remains a significant and potentially high micro-proliferation risk.

The control of services is multi-faceted and due to the already existing wide availability of sensitive information and its diffusion throughout society, the capacity to provide for a ubiquitous suite of regulatory measures is impracticable and more impractically, unattainable. The regulation of services and information, particularly in attempting to ensure compliance and enforce any regulatory measures, would be nearly impossible to apply. As such, any initiatives involving the control of information and services must seek to draw on cooperative, educative and awareness initiatives, rather than those measures that are more coercive and punitively based. The porosity of democratic and open societies, and the potential for this to be abused, was highlighted in the unhindered ability of terrorists to train and develop the necessary skills for

[64] The task of the Office of Film and Literature Classification is to review and classify publications, videos, films and computer games, which are sold or hired through Australia. While most of the effort is directed towards film on the grounds of violence or sex, there is only limited latitude regarding controls of material outside of these areas. The classification systems for video and films, which mandates that these must be a classification prior to sale or hire, is different to the literature classification system which is based on self-assessment (unless a publication is submitted for classification in which case if it is approved for release, no further prosecution can occur). Police and customs can submit material for classification, but it relies on these services identifying the nature of the risk and if the information on the subject matter is already widely available, further restrictions are unlikely to be imposed. The vulnerability within the information regulation process, in which there is currently no controlled environment, is the availability of Internet material, access granted through freedom of information and the increasing availability of de-classified research/information, which is now increasingly publicly available.

suicide attacks against the United States on 11 September 2001. Many of the terrorists had received training in a range of capabilities in the months preceding the suicide attacks, yet despite the names of at least three terrorists within the cells appearing on United States and other international alert lists, the terrorists were able to enter the United States and operate unhindered.[65]

No analysis of reduction counter-measures would be complete without reference to social safeguards and while it is outside the actual scope of this thesis, at least in any capacity to examine in detail, the development and application of foreign and national policies in establishing social safeguards against non-state activity cannot be underestimated. While it is often asserted that intelligence is the first line of defence against terrorism, a strong societal commitment to the rule of law and social justice is the most fundamental of all defences against non-state actions.[66] Yet it is hard to establish a clear social valuation function, at least one with any real meaning, that allows the articulation of a clear and coherent social, economic and cultural strategy, other than the application of fair and equitable laws. Hence, considerations of human rights, civil liberties and fair and non-preferential commercial and government practices, must remain as core values in any attempts to reform and enhance counter-measures and reduce the level of actual risk.

---

[65] This comment follows revelations of the activities of the terrorist network in the months prior to the attack against the United States on 11 September 2001. Flight simulation training was a central theme in the attacks, with a number of the terrorists having trained as pilots prior. For example, Mohamed Atta, widely believed to be the leader of the terrorist cell, received pilot training at Huffman Aviation in Venice, Florida and took two three-hour courses at SimCenter Incorporated in Florida, where he trained on a Boeing 727 full-motion flight simulator. There was also reporting to indicate Atta made inquiries regarding the use, purchase and technical capacity in the aerial delivery capacities of crop dusters. Media reporting suggests the terrorists requested training for horizontal flight, rather than for take off and landing, yet even with these indicators, there were no suspicions raised by the various commercial flight training centres. J. Stewart, 'Iraqi Terror Connection?', *CBS News Report*, Washington DC, 18 September 2001, (accessed 19 September 2001), http://www.cbsnews.com/now/story/0,1597,311414-412,00.shtml.

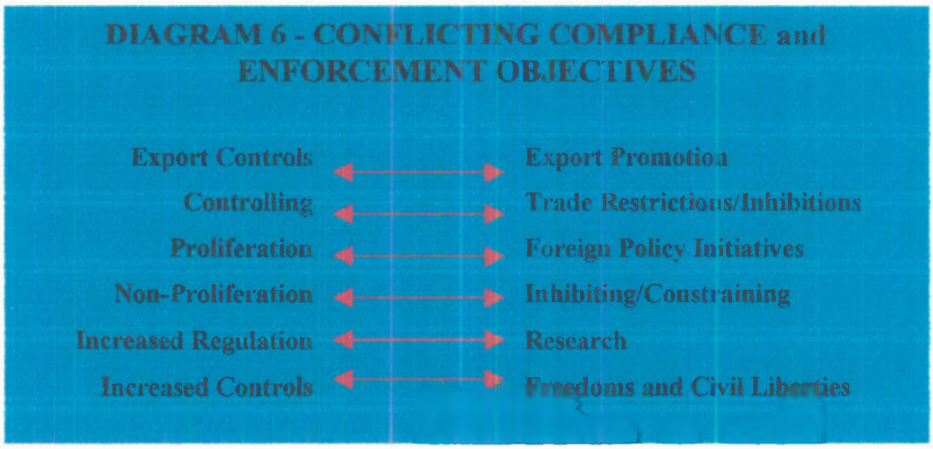
[66] Hope, op. cit., Section 4.45, p 63.

ENFORCEMENT: A STRATEGY FOR DETERRENCE

Enforcing the Risk – Compliance and Enforcement

The inadequacy of enforcement mechanisms exists as a systemic issue throughout nearly all international and national regulatory legislation. Each circumstance is particular to the jurisdictional environment of the state party where any incident may have occurred, the country in which the intended target of the action was located and the nationality of the belligerents involved. Additionally, the various forms of jurisdiction that apply, varies dependent on the state's interpretation of relevance (for example, the context of armed conflict), the requirements for extradition (for example, determination of the nationality of the belligerents) and in defining the actual crime (for example, was it a terrorist or criminal action – which ultimately determines responsibilities for prosecution and jurisdiction).

Providing for adequate enforcement capacities throughout regulatory and legislative structures is a multi-dimensional issue. Firstly, there are those benefits derived from increased confidence within the controls due mainly to the recognition by parties that action will be taken against breaches of any compliance requirements (which includes those intrinsic and extrinsic parties to the breach). Secondly, there is the unambiguous recognition by parties with the intention of deliberately breaching the controls that counter or retaliatory action is assured (if detected) – which in turn exerts an influence on the cost-benefit assessment and the decision to effect a desired outcome by the non-state organisation. Thirdly, and most critically, the chance of detection and interdiction is considerably increased due to better enforcement capacities.



Enforcing compliance imposes conflicting objectives for the state party throughout the regulatory continuum where decisions concerning interdiction, compromise or recognition, must be continually assessed against individual and organisational risk. In state party efforts towards enforcing compliance, considerations of human and civil rights must then be weighed against the opportunity cost of increased security and safety. Diagram 6 represents a summary of the polarisation in objectives where costs must be potentially offset against any potential benefits.[67]

Enforcing the Risk – International Measures

Despite a wide array of seemingly relevant legislation and norms throughout international law, there remains little enforcement capacity other than through the prospect of retaliatory action by states. Nearly all transnational non-state actions, other than the culminating act of violence itself, lacks any context or relevance within the application of international law. International legislative and customary law does not have the micro-controls and judicial organs to enforce non-state activities. Even defining non-state actions which breach international law is often unclear, particularly when it may only concern aspects of micro-proliferation or relatively minor activities involving capability development.

---

[67] The diagram is based on a model represented in the Office of Technology Assessment, *Proliferation of Weapons of Mass Destruction, Assessing the Risks*, p 26.

The actual prosecution of transnational non-state activities under international law, as opposed to the wider issue of enforcement, is an uncertain and ill-defined process, irrespective of the technology applied – conventional or unconventional. The mechanisms providing for the justification of retaliatory responses are too often confused with the legislation that allows for the exercise of prosecutorial and judicial measures. A state's retaliatory response to an act of terrorism through the use of force can more often be easily justified (albeit not always legitimised) through a range of international and United Nations resolutions and mandates, yet the more complex issue of how to prosecute and enforce illegal, criminal or terrorist acts under international law, is based predominantly on theoretical case studies with no precedents or anecdotal evidence. The problem of prosecuting non-state actions within international law is particularly exacerbated by the differently interpreted definitions of terrorism. For example, distinguishing the difference between armed conflict, which depends on how the perpetrator and the target of the attack is classified, defines whether the act is considered by the state party as terrorism or a military operation. Not surprisingly, there have been no precedents in any international legislative actions involving WMD and/or non-state capabilities, regardless of nationality or typology.[68]

As Appendix One of the thesis notes, there is no over arching international convention that deals with non-state actions or the technological capabilities they might develop or employ. There are a range of resolutions that seek to establish the illegitimacy of many non-state acts and the levels of acceptable normative behaviour on the part of states in dealing with actions involving asylum, sponsorship, funding or association. There is, however, no legislated process or judicial instrument that allows non-state actors to be brought to trial or that

---

[68] The League of Nations in 1937 drafted a Convention for the Prevention and Punishment of Terrorism, yet the Convention was never enacted, due mainly to the start of hostilities during the Second World War and wider political considerations. R. Balkin, Prevention of Terrorism: Treaties and Conventions, L. Hansch, *Prevention of Politically Motivated Violence National Counter Terrorism Conference 8-9 November 1994*, Canberra, p 35, and Attorney General's Department, *Press Release – Commitment to an International Criminal Court*, Canberra, 26 August 1998, (accessed on 21 August 2000), http://law.gov.au/aghome/agnews/1998newsag/467_98.htm.

further provides the capacity to prosecute activities that may otherwise have been associated with non-state actions.

There are two international legislative processes that under certain conditions may theoretically be capable of being applied to non-state actions, specifically those involving a violent act of terrorism. The first and most significant of these involves the use of the Rome Statute of the International Criminal Court.[69] The second is the establishment of an Ad Hoc tribunal by the United Nations. It was as a result of the absence of legislative instruments and the requirement to remedy the deficiencies in the Ad Hoc tribunal process that the Statute was actually developed. The International Criminal Court does not provide for an exhaustive code or wide range of legislative measures, maintaining only a limited capacity for the prosecution of transnational acts of terrorism, and then only under very limited conditions. It is primarily designed to take over when criminal justice institutions are unwilling or unable to act.[70] While Article V of the Statute applies the jurisdiction of the Court to crimes of genocide, crimes against humanity, war crimes and crimes of aggression, the Court's relevance to acts of terrorism is limited by definition and the primacy provided to state parties in the prosecution of any acts within the jurisdiction of state boundaries and through national legislation.[71] Furthermore, the overall international opposition to the Court, particularly by the United States, potentially undermines its overall legitimacy and likely effectiveness.

---

[69] The International Criminal Court is due to enter into force on the first day of the month after the 60th day following the 60th instrument of ratification and is not expected to be functioning until 2002.

[70] Scharf avers that the International Criminal Court would have jurisdiction over serious violations of laws and customs applicable to international armed conflict, including the use of poison or poisoned weapons (Hague Convention) or asphyxiating, poisonous or other gases, materials or liquids (Geneva Protocol). This should, at least in theory, also include those acts involving the employment of weapons, and of the persons responsible for intentionally directing attacks against the civilian population, not involved in hostilities, to be held accountable. Scharf, op. cit., footnote 132, p 504.

[71] For example, Article 12 provides that in relation to referrals by state parties or investigations initiated directly by the Prosecutor (defined within the Statute), the Court may only exercise jurisdiction if either the State or the territory in which the conduct in question occurred, or the State of which the person accused of the crime is a national, is a party to the Statute or has accepted the jurisdiction of the Court as a non-state party. Rome Statute of the International Criminal Court dated 17 July 1998, (accessed 9 September 2001), http://www.austlii.edu.au/cgi-bin/disp.pl/au/other/dfat/seldoc/1998/4618html?query=%7e+rome+statute+of+teh+international+criminal+court.

The Statute establishes that it is the duty first and foremost of every state party to exercise its national jurisdiction over those responsible for international crime, including acts of terrorism. The Statute lacks relevancy against most non-state activities as it only applies when the state party is incapable of acting. In most cases of terrorism it is also more probably the strong desire of the affected country to try any crimes within its own territory or jurisdiction. Furthermore, the difficulties encountered by the Government of the United Kingdom in the trial of the Libyan nationals involved in the bombing of Pan Am Flight 103 at Lockerbie, reaffirmed the enduring need for states to maintain national controls throughout the evidentiary and prosecutorial processes involved in the pursuit of transnational terrorists.[72] Additionally, the uncertainty within the trial process imposed through the potential for extensive delays, along with the political benefits derived by a state party which is seen to be imposing harsh punitive measures, collectively inhibits any desire for action in these areas within the current limitations inherent throughout the international criminal judicial system.

The second mechanism for the prosecution of non-state activity relies on Chapter VII of the United Nations Security Council. This involves the formation of an Ad Hoc or international criminal tribunal. This has occurred twice in the relatively recent past, with both cases looking at issues related to war crimes and

---

[72] The downing of Pan Am flight 103 over Lockerbie on 21 December 1988 offers an interesting case study involving the frustrations in and relative ineffectiveness of attempting to prosecute terrorists within an international arena. Albeit, the prosecution (and subsequent dismissal of charges against one of the Libyan nationals) was under Scottish jurisdiction in a Dutch court. As such, the trial was not conducted under international law, however, aspects in relation to extradition and the subsequent sanctions imposed against Libya were. The case study is interesting because Libya refused extradition of the two Libyan nationals accused of the bombing. The Security Council adopted two resolutions imposing sanctions against Libya due to assertions by the United Kingdom and United States, of state sponsorship of terrorist activities. This, however, was not proved. Libya filed two applications for interim relief against the United Kingdom and United States with the International Court of Justice. Libya asserted that as a party to the 1971 Montreal Convention, it was not obliged to extradite its nationals and could conduct the trial in Libya. The International Court of Justice overruled Libya and determined that it was obliged to carry out decisions of the Security Council in accordance with Article 25 of the United Nations Charter. The Convention in essence makes it an international criminal offence to hijack an aircraft, hence, the decision by the Court held that in accordance with Article 103 of the Charter, the obligations of state parties in that respect, prevail over their obligations under any other international agreement, including the Montreal Convention. The Libyans were extradited and stood trial under Scottish law in the Dutch court in 2000, however, the outcome proved frustrating and inconclusive to the United Nations, the Libyans and the United Kingdom and United States Governments. Department of State, Bureau of Diplomatic Security, *Significant Incidents of Political Violence Against Americans*, Department of State Publication, Washington DC, 1998, p 58.

acts of genocide.[73] Not surprisingly, there has always been a strong reluctance to instigate these tribunals and even stronger pressure, particularly from countries such as China, to not convene further criminal tribunals at all.[74] Interestingly, the process can be quite unbalanced as Permanent Members of the Security Council can veto any substantive actions of the Security Council, thereby circumscribing or shielding themselves or their allies from the jurisdiction of the tribunal.[75] It was as a result of frustrations by states in the costs of maintaining these tribunals, and what has also been described as 'tribunal fatigue', that the impetus for the adoption of the Rome Statute for the International Criminal Court was developed.[76] While the establishment and application of an Ad Hoc tribunal system may appear theoretically possible, it would most likely be limited to actions only involving international armed conflict, which by definition and scope then excludes most acts of terrorism.[77] There has been no precedent established for the use of the Ad Hoc tribunal structure against acts of terrorism – national or transnational.

In terms of the capacity to enforce compliance with international norms, (as opposed to prosecution under international law), measures remain limited and can be widely interpreted. The United Nations Security Council has a range of

---

[73] These involved the specific actions in the conflict in the Former Yugoslavia in Security Council Resolution 808 (1993) and in the case of crimes of genocide, it was applied as the Rwanda in Security Council Resolution 955 (1994). As Scharf points out, the two tribunals would also have jurisdiction over, *inter alia*, violations of the 1907 Hague Convention. While Scharf argues, however, that if it applied, it could also include violations of chemical use, this then becomes a very tenuous and entirely theoretical model in which to establish legitimacy, other than through establishing the use of unconventional weapons as inhumane. Scharf, op. cit., p 501.

[74] ibid., p 503.

[75] ibid.

[76] United Nations, *Brief on the International Criminal Court*, New York, (accessed 12 September 2001), http://www.un.org/law/fcc/general/overview.htm.

[77] Despite the United States declaring a 'war on terrorism' following the 11 September 2001 attacks against the United States World Trade Centre and Pentagon buildings, the prospect of applying the processes associated with a United Nations ad hoc tribunal would appear unlikely. While this would mainly be due to issues related to United States sovereignty and the strong desire to prosecute the terrorist actions within the continental United States, it is also less likely because the tribunal would largely be restricted to cases of international armed conflict. The corollary to this is that while even the United States definition of terrorism (as at October 2001), does not include terrorism as an act involving armed conflict, when viewed specifically as an asymmetric threat or threat to the sovereignty of the United States, theoretically a case could be established. The corollary to this is that the act of terrorism was viewed as being perpetrated by a state-sponsor. That is, it involved the alleged perpetrator Usama Bin Laden having received critical support from the Afghani Taliban regime, hence, the justification to define the act as involving armed conflict could potentially be established.

capabilities it can exercise in justifying or legitimising the use of force against any acts of terrorism (and has done so in the past). Articles 41 and 42 of the United Nations Charter in particular, provide for the capacity to restore international peace and security by force if necessary.[78] This capacity can extend from the imposition of economic and military sanctions, freezing of assets, the use of military force or to the extremes of actually capturing persons responsible for violations of international law.[79] For example, United Nations Security Council Resolution 837 authorised 'the arrest, detention for prosecution, trial and punishment' of Mohamed Farrah Aidid, the Somali Warlord responsible for the murder of 24 United Nations troops in 1993.[80] The Security Council can also adopt resolutions to authorise, and thereby legitimise, member nations to use force in apprehending non-state actors. For example, United Nations Security Council Resolution 1189 sought to condemn the

---

[78] Prior to the advent of the United Nations Charter, there was a customary right of reprisal, permitting nations to use military force to enforce international obligations in limited circumstance. The parameters of lawful reprisals were set forth in the *Naulilaa Incident Arbitration decision*. This in essence embodies the basic principles of moral conduct within criminal and international law. In the *Naulilaa Incident* decision, the arbitrators declared that the exercise of the right of reprisals must be based on a motive furnished by a preliminary act contrary to the law of nations. In other words, the use of force is only justified by necessity and it is necessary to consider as excessive and illegal reprisals out of all proportion to the act motivating them. The 1970 Declaration on Principles of International Law Concerning Friendly Relations and Co-operation Among States and the United Nations Charter, means the use of lawful reprisals should no longer remain applicable. While Scharf goes on to distinguish between the use of self-defence and actions taken in reprisal as part of customary law, arguing that it could be justified on the basis of anticipatory self-defence, his argument does not take into account that any action taken, regardless of the mandate used to legitimise it, would potentially still be outside of a United Nations mandate and particularly in its application against terrorism, it would remain difficult to establish legitimacy post-attack, regardless of the basis of the international laws applied. Scharf, op. cit., pp 489-490.

[79] The relative merit of many of these measures is the subject of wide debate, particularly on the basis of the impact they have on civil populations, as opposed to the state regimes or the functions they are meant to be targeting. One of the most interesting examples has been the continuing sanctions imposed against Iraq by the United Nations. The continuing actions of the Security Council, the United States and United Kingdom in particular, has resulted in the marginalisation of many Middle Eastern, North Asian and former Eastern bloc countries, along with significantly increased risks to many Western democracies, arguably for little derived benefit. The impact of the sanctions economically has been significant but the capacity of the measures to curb the capability development of the Iraqi missile and WMD programs is unclear, uncertain and apparently unlikely. The measures taken against Iraq were initiated on the basis of Security Council Resolution 687(1991), which authorised the use of force and sanctions. The Resolution invokes, *inter alia*, the 1925 Geneva Protocol and 1972 Biological Weapons Convention. Resolution 678(1998), was later invoked to allow for the use of force in response to breaches of Resolution 687, which currently continues in 2002. It was these actions and those of the Western Coalition forces in Saudi Arabia that ultimately, however, provided the catalyst for Usama Bin Laden to act, with his cynosure the September 2001 terrorist suicide hijacking campaign in the United States. While there are many other variables also associated with this, the issue is that even the application of sanctions, economic or military, or the authorisation of retaliatory force, will have wide ranging consequences and ramifications that will resonate for years, particularly throughout Islamic countries .

[80] United Nations Security Council Resolution 837 (1993), S/RES/837.

bombings in Kenya and Tanzania through 'imploring nations to adopt all practicable, effective and legal measures for security cooperation to prevent further such acts of terrorism'.[81]

The enforcement of compliance is a limited and often misunderstood application. Justification has often appeared as an after thought in order to legitimise actions taken, rather than being applied as a preventative measure in anticipation of an act. For example, the bombing of Sudan and Afghanistan in 1998 by the United States in response to the East Africa bombings. The use of military action can be confused with considerations of prosecution and the exercise of justice, at least in the perceptions of those parties not directly involved in the incident.

Notwithstanding the international compliance and enforcement measures available throughout international law or the United Nations, the most effective method for prosecuting terrorist activity still remains within the parameters of national legislation. Any actions taken internationally, would depend on clear attribution and absolutely no ambiguity in the nature or origin of an incident. That is, it would have been clearly attributable to an act of terror and would more probably have involved severe consequences (and would have heightened international visibility). Also as importantly, if an act were to be prosecuted within an international forum, there would need to be established consensus and cooperation by all of the state parties involved. These limitations and the inability to act through an Ad Hoc tribunal structure or within the International Criminal Court, particularly when action may only have been limited to micro-proliferation or capability development, suggests that other than through the threat of retaliatory action, there is only a minimal enforcement capability throughout most international norms. The logical conclusion is then that to rely on international regulatory measures or laws for national security, is to place an unrealistic expectation in the capacity of any of these measures.

---

[81] United Nations Security Council Resolution 1189 (1998), S/RES/1189. Also see Security Council Resolution 1269 (1999), S/RES/1269, which calls upon all states to implement fully the international anti-terrorist conventions (refers to the United Nations Convention for the Suppression of Terrorist Bombings). It reaffirms the requirements for states to adopt greater prevention, cooperation, denial of means, adoption of national measures and the exchange of information in the prosecution of terrorism. It does not, however, provide the judicial vehicle to prosecute acts of terrorism, it merely authorises those actions involved in apprehending any belligerents.

While the 11 September 2001 attacks against the United States may potentially precipitate a change in international and regulatory structures to legitimise increased actions against terrorism, such as the freezing of assets, as the current structures are inadequate even for this purpose.[82] Exhortations of the need for greater controls and regulatory requirements, along with tighter monitoring of states actions against terrorism, is an easy philosophy to extol. The reality, however, is that measures rarely go far enough, have the pervasiveness necessary or the legal mandate required. Despite this seemingly obvious need, progressive and effective change would appear as unlikely, at least until states have increased the strength and capacity within their own national legislation.[83]

Despite the obvious limitations, this is not to totally dismiss all aspects of international law when applied to acts of terrorism. Even though prosecution is best exercised within national legislation, the use of international norms to provide for extraterritorial criminal jurisdiction or a universality in the application of measures against inhumane, ultra-violent or any act of terrorism, is the most significant element. That is, those that choose to utilise violence, CBR and/or WMD capabilities in the conduct of heinous acts, thereby become *hostis humani generis* – an enemy of all humankind. For example, while regimes such

---

[82] SC/RES/1378 which covers Security Council Resolution 1378, establishes the legitimacy of actions by state parties in using force in response to acts of terrorism in Afghanistan. The Resolution also reaffirms the legitimacy of actions, such as freezing assets, stopping the sponsorship of terrorist groups and denying terrorists requests for asylum. Security Council Resolution 1378 (2001), SC/RES/1378.

[83] Following the attacks against the United States in 2001, the United Nations Security Council and General Assembly enacted a range of measures in an attempt to compel state parties to adopt and enforce wider measures against the financing, trafficking and sponsorship of terrorism. The key resolutions included:

- Security Council Resolution 1373 (2001), S/RES/1373 – The Resolution seeks to establish international cooperation to combat threats to international peace and security caused by terrorist acts.
- Security Council Resolution 1368, (2001), S/RES/1368 – The Resolution condemns the attacks of 11 September 2001 in New York, Washington DC and Pennsylvania in the United States.

Other key United Nations initiatives following the attacks included increased efforts to pursue participation in various United Nations conventions, such as the Convention for the Suppression of Financing on Terrorism 1999. Additionally, new work by the United Nations Ad Hoc Committee on terrorism has accelerated the development and implementation of two new conventions. The first of these conventions is a Russian proposed treaty against nuclear terrorism (it is unclear whether this will include aspects of non-fissile materials). The second is a comprehensive convention for the suppression of terrorism, which was proposed by India. Most interestingly this Convention seeks to strengthen the existing legal anti-terrorism framework and includes a 'depoliticalisation clause'. This seeks to establish that an act of terrorism involving innocent civilians and civilian targets cannot be considered a political offence (suggesting it could be tried as a criminal offence in an international court). It could be anticipated that this will be strongly opposed by countries such as the United States, Israel and Pakistan.

as the 1907 Hague Convention and 1925 Geneva Protocol provide no mechanism by which any of their requirements can be enforced (or indeed even through which compliance can be determined), they do serve to establish that any act involving the use of these capabilities is in essence illegal or inhumane. While these principles cannot be enforced, particularly given the limited relevance and scope of international law, they can be enshrined as values and determine what is acceptable and what is not within national legislation. In this sense, these values then establish the international standards and degrees of acceptability for individual and collective behaviour, which can then be applied to calibrate the use of specific acts or weapons and also justify any national actions.

Enforcing the Risk – National Measures for Enforcing and Prosecuting Non-State Actions

Recognising the enforcement limitations and the inadequacy of international law to punish non-state activities shifts the emphasis to the ability and capacity within national legislative covers an extensive range of functions. Like international measures, national legislation is multi-dimensional. There are those controls that regulate and ban activities associated with an organisation which seek to impose restraints on the use of violence. There are also those measures that enforce the regulation of the capabilities required to achieve an outcome. While both aspects are inseparable and also critical in determining non-state use and development of CBR WMD capabilities, as with all deterrence measures, success is a question of balance as much as it is the application of any legislative measures.

In the seminal 1979 review of Australian counter-terrorist capabilities, Hope stated that in denying their tools to the non-state actor we potentially render them impotent.[84] While there is a strong basis for this argument, the simplicity of the problem fails to account for the increasing resilience, resourcing and influence changing non-state organisational behaviour has in determining the types and

[84] Hope, op. cit., pp 87-99.

methods of violence applied. Hence, the need for any regulatory structure to include and enforce those measures that establish acceptable behavioral norms is as vital towards the development of safeguards as is the enforcement of regulatory requirements against the misuse of specific risk capabilities. Therein lies the nature of the problem, which is as much a function of any escalation in threat, as it is in the correlation of enforcement measures and norms to public perceptions. Hope's assertion, however, that whatever measures are necessary should only be inculcated within a criminal judicial system as this provides any necessary capacity to enforce compliance, reflects the now anachronistic nature of the assessment and the threat environment of the time. That is, the assumption fails to account for the increased propensity by non-state actors to use ultra-violence and apply more capable and lethal weapon technologies.

Prior to further developing and improving enforcement strategies, it is necessary to define the regulatory environment and context in which the controls are applied. These will of course vary dependent on relative hazards, volumes, licensing and the economics of the application, just as much as it will on the relative risks associated with the various materials, components or processes involved. Enforcement mechanisms can be broadly established within three regulatory categories: self-regulation, legislative mandate and a fully mandated regulatory environment.

It is neither practical nor possible to apply one standardised system throughout the entire processes for each risk material. Rather, where practicable, regulatory structures should be closely aligned to the functions of risk and outcome. Issues such as consumption, synthesis, genetic engineering and production considerations all potentially change the nature of intent, utility and the definitional criteria within the life cycle of materials and equipment, even including the provision of services. The critical issue, however, is one of calibrating risk against specific industries, processes or activities, regardless of the function it is associated with, or ascribed to, such as those within the biotechnology, engineering and chemical sectors. This includes the provision of support or ancillary services contracted to provide specified activities, such as those within certain processes that involves security clearances or self-

assessment. An example is the use of contracted non-government services in the provision of critical security, vetting and clearance processing for risk materials throughout most Australian ports and airports. Low levels of training, devolution of direct responsibilities and low thresholds for staff security checks, all combined with services often being provided by the lowest contracted tenderer, are increasingly indicative of a systemic emphasis on fiscal efficiencies rather than security effectiveness.

The increasing reliance on a culture of self-assessment and self-regulation within the Australia's regulatory framework cannot be sustained in the regulation of the more high risk CBR capabilities. It is indeed one of the more critical structural and systemic failings throughout the method of control and regulation nationally. The case study of the Victorian dangerous goods codes and its regulatory legislation in Appendix Two, highlights the pretence and ineffectiveness within a system reliant on enforcement and compliance but also dependent on self-regulation and self-assessment.[85] While the reality is that fiscal and economic pressures will always be the strongest determinant of the level of any measures to be adopted in the response to risk, the capacity of the industry to sustain and apply regulation is a critical factor in identifying core vulnerabilities. For industries and sectors that are opposed to increased government intervention and regulation, regardless of the considerations of risk, then a legislative mandate may ultimately be the only vehicle through which regulation may be applied and exercised.[86]

---

[85] One of the more interesting examples of compliance, or a lack thereof, is in the customs controls for the management of cargo throughout Australia air and seaports. Customs officials estimate that there are 1.6 million containers which enter Australia annually. Further estimates suggest that no more than one percent of these containers are checked (it is likely the estimate for clearances is an overly optimistic assessment with the reality suggesting it is closer to 0.1 to 0.3 percent). In terms of the capacity to enforce the regulatory requirements for cargo, Customs report that there are very low levels of compliance and that as a service they lack an effective process for recognition of high risk cargoes entering Australia. The capacity to enforce compliance is predominantly administrative, being limited to pecuniary penalties (for those not involved in illegal activities but in breach of compliance requirements for timeliness, identification etc.). Customs reports that there is also little capacity throughout the existing legislative and regulatory requirements to enforce imposed reporting requirements for cargo. Australian Customs Service, *Preliminary-Principles for Administering Proposed Penalty System*, Customs Legislation Amendment and Repeal Bill 2000 (International Trade Modernisation), (accessed 2 August 2001), http://www.customs.gov.au/cmr/cmr_penalty/contents.htm. Also personal communication with Mr B. Hicking, Customs Corporate Relations, Australian Customs Service, 29 August 2001.

[86] The example that best illustrates the pressure exerted by industry sector lobby groups involved initiatives by the Victorian Government in the wake of the 1991 Coode Island contamination accident, for major regulatory reform. The State sought to significantly increase regulatory control and compliance

The ideal for increased national security and greater regulation is to apply a mandatory regulatory environment throughout all private, public and government areas and processes involving risk CBR capabilities. Such a regime would, however, be impracticable, excessively costly and unsustainable in resources, certainly within the medium to long term. While there would be extensive pressure and resistance against increased regulation throughout many industry, research and government sectors, such as those within the biotechnology research industries and chemical sectors, the fact is that regulatory legislation often already exists. Albeit, many of these current systems are applied with varying degrees of success due to a lack of enforcement, monitoring or surveillance practices. As has already been identified, increased enforcement may not necessarily only be achieved through the introduction of new legislation or the application of harsher punitive measures, it is as much a process of education and inculcating reporting and regulatory functions as standardised activities throughout industry, as it is in establishing the mandatory requirement for ranges of reporting, monitoring and security. In essence, greater enforcement capabilities can be encapsulated through three broad areas: increases in the efficacy and the capacity of existing controls, greater control and coordination across the spectrum of regulatory measures and the introduction of new and strengthened regulatory legislation.

Enforcing the Risk – Efficacy of Controls.

Efficacy throughout the range of controls depends not only on the efficiency in the application of measures, but also in ensuring controls have the necessary specificity without constraining their application to only a few narrow environments or outcomes. This is achieved through clear and unambiguous

---

requirements, however, most of the efforts by the State Government eventually became moribund following intense pressure by the Victorian chemical sector. The comments, however, refer more significantly to current initiatives to regulate the biotechnology sector. Over the last five years in particular, there has been a wide range of self-interested and industry lobby groups attempting to exert pressure on the Commonwealth Government. These pressures were heightened following the December 2000 introduction of the Gene Technology Act 2000, where groups were increasingly concerned over government restrictions which may potentially impact on research, trade and commerce throughout the sector.

definitional structures that apply throughout the regulatory continuum as well as uniformly across the various jurisdictions. Efficacy is also reflected within the different regulatory environments where unlike the example cited on the Victorian Dangerous Goods case study (see Appendix Two), the level of risk should be reflected by a commensurate level of control. For example, where voluntary or discretionary reporting and notification structures are applied, there should still be a range of redundancies, either through the use of duplicative processes or measures integrated throughout other mandatory legislative requirements.

Ensuring compliance is as much about change within work practices and organisational cultures, as it is in the enforcement of compliance through the application of punitive measures. For example, the culture of enforcement, or lack thereof, that existed within the Victorian case study of dangerous goods legislation in Appendix Two, involved an accepted and enduring organisational culture involving the minimisation of the impact of regulatory requirements, as opposed to facilitating their enforcement, throughout Victorian industry and government. The current culture throughout most of those sectors involving the national control and regulation of CBR risk materials, equipment and services, particularly in how compliance is enforced, would require a paradigmatic structural shift if required capacities are to be increased. Currently regulatory structures too often only maintain the capacity for the collection of excise, duties or revenues, more often correlated to licensing, accreditation, capacity and volume thresholds, rather than the requirement for enforcement and calibration of risk.

Enforcing the Risk – Control and Coordination.

A fundamental failing in the capacity to enforce compliance throughout nearly all regulatory structures is a lack of coordination and control within, or of, the process. A large part of this is attributable to the diminishing role of the Commonwealth and the subsequent lack of uniformity throughout the eight jurisdictions. The common denominator throughout the more successful regimes that enforce and apply compliance standards uniformly is, *inter alia*, the role of

the coordinating and/or inspectorate instrument. For example, the international standards and regulatory requirements specified and enforced by the International Atomic Energy Agency for the control of fissile materials, provides one of the most proactive, preemptive and successful inspectorate and control regimes, which incorporates widely exercised interventionist, compliance and enforcement protocols.

While the relatively low risk of many of the CBR material regulatory structures neither justifies nor demands draconian enforcement capacities, the requirement for proactive and responsible coordination of control measures still remains critical. The international coordination, technical secretariat and policy agency for the Chemical Weapons Convention, the Office for the Prohibition of Chemical Weapons in the Hague, provides a range of overarching regulatory functions at the international level to assist states in their compliance requirements, which is unlike any other regulatory regime. The most interesting aspect to the regime, and one of its greatest strengths, is the requirement for a national regulatory body to oversee coordination, advice and compliance requirements. These functions are provided by the Australian Safeguards and Non-Proliferation Office, which is responsible for enforcing all compliance requirements set out in the national legislation – the Chemical Weapons (Prohibition) Act 1994. The use of a regulatory office appointed as a statutory organisation is unique within an Australian regulatory environment, particularly when its extensive powers and range of penalties are compared to regulatory legislation, such as the Therapeutic Goods Administration Act 1989. Most notably, the capacity to inspect facilities and the requirements for the reporting of specific trade, research, production and disposal action for many high risk chemicals and their precursors, provides the Office under the Chemical Prohibition Act 1994, with an extensive enforcement capacity.

While there are still inadequacies within the enforcement capacity of the Convention, both at the international and national levels, the regulatory and coordination structure do provide an effective coordinating and implementation model on which to base other national regulatory systems, particularly those that may involve any range of certain dangerous goods or equipment (and not just

those limited to international regulatory requirements). Most significantly, it is the responsibility of the national Safeguards Office to coordinate specific aspects of technical advice and enforce mandatory reporting and declaration criteria by industries within the Convention. It is via the empowerment provided for in the Chemical Prohibition Act, through a clearly articulated legislative mandate and the ability to demand active reporting requirements from industry, that the relative success of the Chemical Act can be attributed (at least when compared to other regulatory systems).

The utility, structure and mandate of the Safeguards Office offers significant potential for the development and implementation of other national regulatory measures, most particularly those throughout the biotechnology sector. Even the regulation of the biotechnology sector could easily be enhanced with a legislative mandate incorporating a range of additional security requirements, particularly if it was under the auspices and intent encapsulated in the 1972 Biological Weapons Convention (despite its current inability to be applied to non-state, and most state, activities). As the Convention is already enacted through the Commonwealth 1976 Crimes Act, the Government does not need to await the finalisation of any initiatives by the Ad Hoc Group (which as at early 2002 had stalled), to further increase the capacity of the Convention or its national legislation. There is significant potential, and indeed a clear justification, to build on already identified initiatives and increased regulatory criteria, even outside of the immediate requirements addressed in part by the Ad Hoc Group. While the Ad Hoc Group has attempted to consider a wider range of additional reporting, monitoring, surveillance and enforcement criteria, whatever the resolution, they will not go far enough in satisfying any non—state national security requirements.

Following the 11 September 2001 terrorist attacks in the United States, the United Kingdom as an example, has already initiated action to increase the capacity of its own biological regulatory legislation, which was based largely on the Biological Weapons Convention. Changes have sought to dramatically increase clearance, handling, security and access to biological materials, which includes wide reporting and monitoring functions, yet none of these

requirements are reflected within the Biological Weapons Convention. The question remains then as to why Australia should not initiate similar, or even greater, regulatory action to provide for increased control throughout its national biotechnology sector.

Table 15 – A National Initiative Proposed Increases to National Biological Regulatory Legislation

- Measures to further define risk on performance based outcomes rather than materials based outcomes.
- Increases in the licensing, accreditation of biotechnology facilities.
- Increased facility security requirements to include staff, visitor and liaison personnel checks.
- Facilities involving work in BSL 2, 3 or 4 containment would require significantly tightened accountability, reporting and end-use verification processes.
- Measures better defining the establishment of misuse.
- Escalating punitive measures to apply across the spectrum of use to include acquisition, production, stockpiling, weaponisation and (micro) proliferation.
- Measures to establish the requirements for sampling, testing and the designation of statutory 'experts'.
- Wider legislative powers in the application of measures from individuals, companies and to other state parties.
- Ubiquitous and mandatory security measures for all procurement, sale and research tasks.
- Increased obligations on producers and distributors of biotechnology materials, equipment and services.
- Education and service provider declarations and obligations for all non-national research and commercial work. To include tightened inspection, monitoring and third party clearances.
- Wider reporting, monitoring and surveillance criteria for industry and research covering all production, distribution and sales.
- Increased dangerous goods handling, transport, storage, reporting and disposal reform.
- Establishment of a statutory regulatory body for all national biotechnology services.

Changes in many of the processing, handling, security and definitional criteria across the Australian legislation that underpins the Biological Weapons Convention would undoubtedly result in significantly increased security benefits, along with a potentially major reduction in the residual risk inherent throughout many activities within the sector. Albeit, any initiatives would require new legislation as the Crimes Act, at least as it currently stands, fails to incorporate the requirements for ubiquitous and mandatory reporting, monitoring and surveillance, or indeed many of the other further requirements that would be necessary to strengthen any national application. More critically, the existing legislation would require such major reform due to its weak definitional framework and the lack of any enforcement capacity, that completely new legislation incorporating many of these considerations may be the only practicable solution. Table 15 reflects those changes, that at a minimum, would be necessary to heighten the security posture throughout the national biotechnology sector, either as new legislation or through major reform to the existing Commonwealth Crimes Act 1976. This reform, when combined with the coordination and enforcement provided through the appointment of a regulatory authority, such as the National Safeguards and

Non-Proliferation Office, could provide for a significantly increased biotechnology regulatory environment.

Enforcing the Risk – New Regulatory Controls

The reliance on a criminally focused judicial system, is convenient and provides for the appearance of relevance and acceptability. However, if not adequately structured and applied, it may be insufficient to attempt to apply escalatory levels of enforcement and regulation against what are often discrete indicators and widely different evidentiary signatures. Structurally, the existing system lacks any actual capacity to extend beyond criminal acts, is inadequate in enforcing technical requirements specific to capability development and is only capable of being applied against the regulatory requirements to restrict certain aspects of state-based WMD proliferation. These factors, when combined with what is an elephantine and blunt judicial structure, suggests that ad hoc changes and amendments to much of the current regulatory legislation, have eroded and undermined its capacity and application. These considerations, along with the need to integrate the requirements of other chemical and biological micro-regulatory and anti-terrorist measures, stretches the flexibility and capacity of current legislation well beyond what was ever envisaged in its application or relevance. Hence, new legislation, in which many of these direct and peripheral issues can be swept up in, would appear necessary and is one of the few ways in which the

Table 16 – Minimum Criteria for Proposed National Non-State WMD Legislation.

- Clear and unambiguous definitional criteria.
- Wide ranging application against WMD throughout the spectrum of activities, to include aspects of threat, development, use, micro-proliferation and hoax activity.
- Performance based outcomes with capacity for wide interpretation of intent, capability, threat and utility.
- Defined evidentiary and processing criteria.
- Increased punitive and security measures across the range of escalatory activities.
- Classification and categorisation of risk dual-use activities, materials, equipment and services.
- Defined security criteria for personnel, access, handling, facilities, and compliance criteria (to include notification obligations).
- Extradition and status of non-nationals.
- Clearly defined legislative structure at the Commonwealth and throughout the jurisdictions, to include inter-relationship with BWC and CWC national legislation (or other relevant acts and regulations).
- Inclusion and/or correlation of national regulatory criteria for non-WMD chemical, biological and radiological materials, equipment and services, for example, dangerous goods codes.
- Reporting, surveillance, monitoring and compliance obligations on producers, distributors, sales and possessors.
- Facility security compliance and handling requirements.
- Establishment of an administration body and regulating authority, to include agency/department responsibilities.
- Criteria for provision of services, information, funding, assistance and associated activities by single or multiple parties involved, directly or indirectly.
- Obligations on service, information, equipment and materials producers, distributors and vendors.

definitional specificity necessary can be used to further target the full spectrum of escalatory capabilities.

For any new legislation to have any real impact requires a shift within existing regulatory paradigms. Emphasis on export regulation, punitive measures and a reliance on the criminal judicial structure, must now be increased in scope to include measures that incorporate more active counter-proliferation strategies and the wider ability to enforce controls. This would also need to include a wider scope in the legislation and most importantly, greater flexibility and specificity in defining the nature of what is to be controlled and regulated. For the most effective and widest ranging changes to how CBR regulatory capabilities are to be controlled, it is necessary to consolidate as many of the different processes into one single, uniform, national legislative regulatory structure. The effectiveness of these measures, however, depends not only on their adoption, but also the need for their ubiquitous implementation. Table 16 provides an outline of those minimum criteria necessary to strengthen the control of WMD capabilities – non-state and state. Whether this is effected through a suite of multiple acts or regulations, is irrelevant. What is important is the need for the Commonwealth to adopt uniformity and enforce the required measures throughout all the various jurisdictions.

Enforcing the Risk – Extradition

One of the key aspects of the enforcement of national and international law is the issue of extradition, particularly given the strategic nature of micro-proliferation activities by transnational terrorist organisations. In order to extend the capacity of any national legislation, it is necessary to be able to apply the legislative processes as widely as practicable, without being limited by geographical and/or state boundaries. This is of course always best facilitated through diplomatic and cooperative international extradition agreements, normally achieved through bilateral or multilateral arrangements between states, but the reality is that these are not always achievable. While Australia maintains a range of these extradition agreements, in the main articulated within national legislation through the Australian Extradition Act 1988, at best extradition still remains

more a quasi-judicial process than a prescriptively legislated function.[87] While it involves a range of laws and generally rests on the existence of a treaty, this in itself, however, is not a pre-requisite in securing the return of a non-state actor.

There are a range of legal principles which need to be satisfied prior to establishing extradition, however, there is no fundamental rule to guide the application of any extradition requirements. Extradition is dependent on complex legal principles and each request is determined by the nature of the crime, the nationality of the responsible party and the country to, and from, where extradition is sought. For example, extradition is largely determined by the 'double criminality test', which broadly establishes the legitimacy of the extradition request by determining whether the crime for which a person is requested for extradition is also considered a crime in the country of refuge. If one country imposes capital punishment, yet the country of refuge does not, a complex situation can develop with little prospect of any satisfactory resolution. Despite these technical legal hurdles, the requirement to extradite for illegal transnational activities, is a crucial component within any national suite of counter-measures. This identifies a clear need and priority for Australian foreign policy to strive towards more effective bilateral and multilateral extradition agreements regionally, particularly given the increasing non-state proliferation potential in conventional and unconventional weapons.[88] The fundamental premise, however, against which all extradition is calibrated continues to be based on the universality of the crime for which the extradition process is sought. Consequently, Australia's continued and active participation in establishing international counter-terrorism normative practices remains a critical element in the development of national and international extradition policy and legislation.

---

[87] The aim of the Australian Extradition Act 1988, is to codify the laws relating to the extradition of persons from Australia to extradition countries. In particular, it is to provide for proceedings by which courts may determine whether a person is eligible to be extradited, without determining the guilt or innocence of the person of an offence; to facilitate the making of requests for extradition by Australia to other countries and to enable Australia to carry out its obligations under extradition treaties. Commonwealth Extradition Act 1988, (accessed 12 July 2001), http://www.austlii.edu.au/au/egis/cth/consol_act/ea1988149/.

[88] Office of Secretary of Defence, Proliferation: Threat and Response, pp 21-30, 61-66. Also see Central Intelligence Agency, op. cit., pp 1-11.

DETECTION: A STRATEGY FOR DETERRENCE

Detecting the Threat

At the crux of the issue of detection of non-state capabilities is the capacity to calibrate and estimate risk. Yet the issue of detection, particularly in a context of its deterrence value, is critically about collection, processing, analysis and assessment of information, rather than just an ability to sample, monitor or analyse CBR materials. This thesis has deliberately gravitated away from an exercise in the evaluation of the latest technical capacities and technologies in the detection of CBR or explosive materials. These capabilities remain only a very small aspect in the wider capacity to detect non-state activity – conventional or unconventional.

It is the process of information management, or lack thereof, that in part defines any detection capability. Without the ability to detect specific trends or patterns of activity, exposure to risk inevitability increases. No more so is this evident than in the limited capacity throughout the Australian security and regulatory environment to calibrate and estimate risk. As established in Section Two of the thesis, current information collection capacities throughout the Commonwealth, States and Territories are severely limited, due mainly to a lack of utility, specificity and veracity, indicating they are unlikely to reflect wider trends and patterns of non-state activity. This difficulty in the capture and processing of information is best represented through two key considerations. The first issue is the need for uniform national categorisation and standardisation of reporting CBR and WMD incidents and capabilities throughout the jurisdictions and at the national level. The second is the mandating of the requirement and processes for the coordination and reporting of notifiable WMD and/or CBR incidents, without which the capability to move towards a uniform national threat and risk analysis is already compromised.

It is the reporting functions and capacities facilitated in the main through monitoring and surveillance, that are central to the ability to detect, and ultimately manage any information requirements. Functions such as monitoring

and surveillance contribute significantly to the collection and verification of information, however, the challenge is also in ensuring that there is specificity in not only the collection but also processing of data. In many cases the processes and mechanisms to pervasively collect and also analyse information already exists, yet is either not realised for its full potential, is misused or is not applied to the control of CBR risk materials. An example is the current regulatory framework for assessing, categorising and controlling risk chemicals. A range of national frameworks includes the dangerous goods codes, poisons schedules and the structures for assessing, classifying and managing agricultural, veterinarian and industrial chemicals.

Many of the existing regulatory regimes, however, do not adequately consider all the necessary aspects throughout the risk continuum (in the context of deliberate misuse), or are not supported through a legislative mandate to operate in such a capacity. The culture throughout the regulation of CB materials, that end-use or disposal is finalised at the point of sale, suggests that without a shift in the structure of research and commercial activities, there will always be a indeterminate element of risk prior to and beyond the point of sale. Hence, the requirement for increased end-use and disposal verification processes, such as those applied throughout the various hazardous waste legislation and in the control of invitro-fertilisation and sports drugs, should be further adopted as a standard industry practice.

The reporting structures and assessment authorities, such as those within the National Regulatory Authority and National Industrial Chemicals Notification and Assessment Scheme, which are used for assessing controls on chemicals within the Australian Inventory of Chemicals and for the Priority Existing Chemicals lists, provide for a wide ranging capability to increase the control of risk chemicals nationally. The inclusion of identified risk chemicals and the establishment of wider ranging criteria for the security, handling, transport and access of many chemicals under the different regulatory schemes [covered mainly by the Industrial Chemicals (Notification and Assessment) Act 1989 and the Agriculture and Veterinary Chemicals (Code) Act 1994], offer the capacity

to more tightly regulate many high risk chemicals, particularly beyond the point of sale.

The corollary to the discriminatory detection processes applied throughout the regulation of chemicals, is a lack of any of these same measures throughout the developing biotechnology sector. This further builds on the earlier point regarding the need within the biotechnology sector in particular, to shift the focus in regulation to performance based outcomes rather than attempting to control capabilities through defining specific materials, equipment or services. While a key element in the coordination of any regulatory regime is in how it is established, and as importantly, how it is enforced and managed, those regimes which are exercised through a mandatory regulatory authority, often appointed and empowered through a range of implementing legislation, appears as the best national vehicle through which to implement and ensure further compliance requirements.

Regulatory authorities, which are often responsible for a range of management and enforcement issues, largely determine the success of any regime's capacity and ability to detect illegal or covert activities. The lack of an overarching regulatory authority throughout many sectors, most particularly in the biotechnology industry, at least one with the necessary mandate and capacity to act, is probably one of the more significant limitations.[89]

Ultimately the end state desirable in attempting to enhance the control and regulation of all the CBR capabilities is based largely on the capacity to process all relevant trade and research activity, whether as a function of production, distribution or sales. Just as critical is the ability to detect any defined activities

---

[89] Section Four of the thesis provides details of the different regulatory structures and processes for biological capabilities. Recent emphasis on genetic engineering and its uses and applications has resulted in the development and introduction of the Gene Technology Act 2000. There are a range of relatively new administrative bodies responsible for advice, regulation and the control of gene technologies, such as the Genetic Manipulation Advisory Committee and the Interim Office of the Gene Technology Regulator (which is the only regulatory body and is a branch of the Therapeutic Goods Administration within the Department of Health and Aged Care). In terms of the micro-biological regulatory bodies, there are a range of advisory boards and government bodies, most notably Biotechnology Australia (which is a non-regulatory body and multi-agency [five departments] service). Commonwealth Scientific and Industrial Research Organisation, *Gene Technology in Australia – Current Australian Research*, Canberra, 15 September 2000, (accessed 12 January 2001), http://genetech.csiro.au/safety.htm.

that fall within specified collection parameters. Detection through the capture of reporting must not only be ubiquitous, but it should also provide for depth throughout its structure and ideally would apply to all designated risk micro-regulatory processes, regardless of threshold, volume, ratios, consumption or processing.

Imposed requirements would undoubtedly be reflected in industry operating costs, yet with the adoption of more efficient regulatory practices and the benefits derived from an increased preemptive security environment, many of these costs could potentially be offset, at least partially. The ability to minimise the impact and costs to industry requires as many existing regulatory and information platforms be utilised as practicable. While increases to the posture in national security preparedness are rarely cost neutral, upgrades and increased capacity within existing operating and regulatory systems, financial assistance and educative programs are just some of the measures that may in part mitigate the impact and potential costs associated with reform. The information platform which undoubtedly offers the greatest potential to detect activity, and which is already pervasively utilised throughout commerce and government, is the Internet.

Detecting the Threat – The Internet

The hardware and software systems that facilitate the collection and processing of information still do not provide the framework that imbues the data with any real utility. The need for wide reporting, monitoring and surveillance capacities is a familiar cliché, however, implicit within the requirement is the need to process and secure any data collected while still maintaining its utility and purpose, that is, to strengthen the regulatory requirements and enforce increased control of CBR and WMD risk capabilities. Despite the availability of various information processing frameworks, the vehicle through which this is possibly best achieved is then, not surprisingly, the Internet. The widely available and pervasive nature of the service, along with the minimal hardware costs, suggests that along with an already established electronic business structure existing throughout most medium to large sized industries, the Internet is the likely

vehicle through which to achieve an integrated and industry-wide suite of information exchange and collection protocols.

It is beyond the scope of this thesis to examine the electronic business capacity of the Internet in any detail, other than recognising its capability and the potential to provide for increased visibility of trends and the analysis of production, distribution, and sales reporting. Already existing Internet information platforms and structures, such as the Technology-Enabled Relationship Management System, provide many of the already widely recognised software processes necessary to further develop any information collection and exchange protocols. The Technology-Enabled Relationship Management System in particular has web based multi-way communication features and traceable connection technology, which already allows for the collection of information on trends, behaviour and technologies (based on micro-marketing strategies).[90] Business to business service industries also rely on these framework systems and utilise a range of protocols incorporating electronic intermediaries, back-end information systems and electronic data interchange.[91] In essence, these electronic collection and dissemination systems are widely integrated throughout many of the biotechnology and chemical production industries. In this sense, they then provide for an already established capacity, at least compared to manual reporting processes, to assimilate data collection and analysis tasks into already existing information capture and collection networks and structures.

Detecting the Threat – Detection Capabilities

While the issue of the varying range of technical capabilities in the detection of CBR materials will not be further addressed, the need to strengthen and increase

---

[90] G. P. Schneider, and J. T. Perry, *Electronic Commerce*, Course Technology Publishing, Canada, 2000, pp 258-261.

[91] Electronic intermediaries provide for greater efficiencies in the capture of data from intermediary sources. Back-end information systems are used through work flow and database management systems and rely on a supplier orientated marketplace. Finally, one of the more important protocols is the electronic data interchange in the exchange of specifically formatted standard business documents, such as orders, bills, credit shipping notices and confirmation of supply. It is a system predominantly used for high volume and repetitive business transactions and is necessary to convert the proprietary data into standard formats. H. M. Chung, J. Lee, D. King, E. Turban, *Electronic Commerce: A Managerial Perspective International Edition*, Prentice Hall International Inc, New York, 2000, pp 201-204.

the analytical detection capacities at various stages throughout the national barrier controls is a crucial aspect in any effective deterrence strategy. Yet consistently the detection or identification of illegal cargo and people movements, both personal and commercial, is largely dependent on visual observation, contact explosive detection, movement declarations or increasingly, self-assessment declaration processes.[92] The capacity to detect particulates, micro-organisms or radioactivity, while a critical function, is too often represented as the solution to the problem of countering non-state CBR WMD capabilities. Technical detection will always be a slave to the limitations of the equipment, either as a function of portability, utility, or simply through the scientific constraints in the detection capacity of the equipment. Detection, however, is a multidimensional deterrence function and while it cannot depend for its entirety on any technical analysis capability, neither can it on guards, alarms or other discriminatory detection processes, for which there are no guarantees that they cannot be circumvented or overcome.

While there are a range of chemical traces and signatures that could theoretically be introduced to assist in tripping detection systems, the potential for interdiction it is still reliant on the training, equipment and capacity of the barrier processing

---

[92] The issue of self-assessment in the management of cargo by Australian Customs, both as unaccompanied baggage and as commercial cargo, provides an interesting profile of the increasing reliance, and limitations, of self-regulation and self-assessment regimes. While Customs has moved towards greater document and record retention obligations, along with increased audit powers for compliance, the precept on which the devolution of regulatory responsibilities is based, proposes that with greater self-regulation comes increased pecuniary penalties. Yet along with other national and jurisdictional self-regulatory structures, what is not addressed is the opportunity cost in security. Rather, it is the benefits of reduced resources and greater efficiency that are widely extolled. The change towards-self assessment in the processing of cargo management by Customs is part of a suite of provisions aimed at modernising the ability to impose penalties within the requirements of the Customs Act 1901. These new measures are to be included as part of the forthcoming Customs Legislation Amendment and Repeal Bill 2000 (International Trade Modernisation).

systems throughout the immigration, customs and quarantine services.[93] The ability to physically detect CBR materials and explosives, along with recognition and identification of equipment and technologies, is an implicit function within any deterrence strategy, yet increasingly this requirement is compromised by fiscal and resource constraints.

RESPONSE: A STRATEGY FOR DETERRENCE

Responding to the Risk – A Balanced Perspective

> It is important that governments are well prepared to deal with terrorist incidents. Lack of preparation increases the likelihood of over reaction. A clumsy response by government to natural disaster cannot encourage its repetition. Clumsiness in handling a terrorist incident is likely to do so.[94]

The need for balanced response measures throughout the crisis and consequence stages of an incident is of course a critical component towards a state's preparedness and capability to act against a threat. It is also just as important in shaping the efficacy of any national security strategy through its underlying deterrence value. There already exists a wide array of published material on crisis and consequence management so this will not be further addressed as a

---

[93] All CBR and explosive materials can be detected, however, the utility and capacity to do this outside of the laboratory environment is difficult. Time and resource constraints, along with most personnel having limited to negligible proficiency in non-organic chemistry or micro-biological work (such as the people who might be envisaged would operate these types of systems), means that detection at the barrier nodes, other than through more obvious measures, is unlikely. There have been a range of detection options examined to enhance detection capabilities, such as the use of taggants (the subject of explosive taggants is examined in Section Four to the thesis), however, as with most detection capabilities, these still remain limited in their overall utility. One proposal has been for the introduction of Carbon-13, a stable and non-radioactive isotope, as a taggant in chemical warfare agents and their precursors. The difficulty is, however, similar to the use of taggants in explosives, it remains potentially uneconomical, unenforceable and technically not viable. Additionally, the use of taggants in some chemicals and most biological materials would be scientifically difficult to achieve and in the main is impractical due to economic and resources implications. G. W. Parshall, 'Scientific and Technical Development and the Chemical Weapons Convention', in *The Chemical Weapons Convention*, ed J. B. Tucker, Monterey Institute, Washington, D.C., April 2001, p 57. Also personal communication with Mr R. Mathews, Defence Science and Technologies Organisation, 12 June 2001.

[94] Hope, op. cit., Section 3.45, p 40.

specific issue within the scope of this thesis. However, the deterrence value within the response function itself, does warrant further analysis.

Crisis and consequence management functions are directed at those activities just prior to, during and following an incident, and as such the deterrence value of any response capabilities will be defined more by aspects of potential. That is, by developing an effective response capability, a state seeks to positively influence the cost-benefit analysis of the non-state organisation, both collectively and individually, in dissuading them from attempting to act because of the inability in achieving any significant outcome. The psychological value attributable to the awareness by the non-state organisation of any deterrence value is of course a rather ephemeral and indeterminate aspect in the deterrence structure (as opposed to the psychological value derived by the government and public). In essence, the juxtaposition is similar to the capacity and ability to measure the effectiveness of national deterrence strategies against non-state actions in that defining an outcome is premised on proving an action or value which is impossible to prove.

The capacity of any response value to influence non-state decisions and behaviour is dependent on a wide range of variables. The real value in any response capability is more likely to be realised within the non-state organisational dynamic. This is through the identification and realisation of the potential of any preemptive capacity, such as those applied through awareness and security training provided to security elements. Yet the dilemma in what information it is necessary to advertise without compromising security aspects of capability is complex and best highlighted in the disparity and response to WMD threats by the United States and United Kingdom governments. The United Kingdom releases little public information on preparedness, yet the United States maintains transparency throughout many of its policy, threat and risk analysis

processes and response activities.[95] Previous attacks against the United States, particularly those directed against the World Trade Centre and Pentagon on 11 September 2001, would appear to suggest there is little deterrence value to be derived from the maintenance of any seemingly capable response force. There is of course a far wider interplay of variables that have influenced these examples, yet the fundamental conclusion is that to the determined belligerent, all response measures can be overcome as in the end it is only a function of scale.

As Kupperman stated nearly three decades ago, 'terrorists change losing tactics'.[96] Clearly the terrorists that attacked the United States, however, did identify key vulnerabilities and a lack of response capabilities to counter existing measures simply through the decision to act in the hijacking and the crashing of aircraft into multiple targets. It was potentially this capacity to act unfettered and with little risk of interdiction, that ultimately influenced the terrorists' own cost-benefit analysis. The capability to deliver a vehicle bomb or release CB agents against relatively secure (to specific types of attack) targets, such as the Pentagon, while not impossible, was clearly a factor considered in the course of the action and method of delivery selected.[97]

Response capabilities, as evidenced by the attacks against the United States, provide little in the way of any assurances, other than against recognised threats. The key to the efficacy in any response capability, or its deterrence capacity, then appears to be as much an element of surprise and timeliness, as it is the effectiveness and efficiency of the response itself. Hence, the need for

---

[95] The issue of how much information should be available has been an enduring subject of wide debate. Emergency Management Australia, a service within the Australian Attorney General's Department, is responsible for the coordination and facilitation of consequence management at the Commonwealth level (and for facilitating Commonwealth support throughout the jurisdictions). Paradoxically, the attempts to educate and warn the public may also be responsible for the increased proliferation of hoaxes as an indirect consequence of a better informed public. Hoaxes have predominantly been targeted at well known and identified societal vulnerabilities, more often countering many of the same perceived benefits that might be considered to have been accrued through a more 'security aware' public. Additionally, the capacity to compromise capability through publicly exercising and responding to hoax incidents (in terms of known response times, types of response and levels of deployment), will ultimately erode many of the well established response capabilities, and as a consequence heighten societal vulnerabilities to these incidents.

[96] Kupperman, *Facing Tomorrow's Terrorist Incident Today*, United States Department of Justice Law Enforcement Assistance Administration, United States Arms Control and Disarmament Agency, Washington, DC., 1977, p 9, as cited in Hope, p 39.

operational security, along with an inherent flexibility and capacity to respond to a wide range of changed threat environments, is a key determinant of the deterrent value of the response, as is simply the ability to respond itself.

CONCLUSION

The analysis of non-state actors and the projections of patterns and trends is an incomplete science and as a body of knowledge there is often little more than inductive reasoning to support assessments. Arguably there is even less to support counter-strategies and how governments should respond to these changed asymmetric threats, particularly when correlated against concepts of deterrence and uncertainties in how to actually respond. There are few studies on these wider issues of non-state action, and none on CBR WMD capabilities, by which theories can be validated or against which empirical data can be collected – at least with any real accuracy. Too often theories operate in a rarified atmosphere as an entirely theoretical or hypothetical model, relying on anecdotal evidence or based on misperceptions influenced through media or funding opportunities. Yet the absence of credible sampling and well defined precedents against which to calibrate counter-measures cannot be used to mask the lack of efficacy throughout existing, or further, deterrence initiatives.

Deterrence is a far more ephemeral and complex issue than crisis or consequence management, yet throughout the evolutionary development of Australia's counter-measures against non-state actors, it has remained a largely ignored concept.[98] A lack of political and social imperative, along with a limited understanding of non-state organisational models and how to best exercise control through the blunt instrument of legislative reform and while still constrained within a criminal judicial structure, has resulted in few efforts of any

---

[97] D. Eisenberg, 'Airline Security – How Safe Can We Get?', *Time*, 24 September 2001, pp 77-81.

[98] This view refers to the consistent findings from Hope, Holdich, and Honan. These reports, all commissioned by the Commonwealth Attorney General, observed that there was a distinct lack of preemption and prevention in the measures applied by Government in attempting to deter acts of terrorism. Interestingly, while the reports all consistently acknowledged the limitations in the development of these measures and the lack of capacity to estimate and calibrate the relative effectiveness of deterrence measures, they all reaffirmed the criticality of a deterrence strategy throughout any national counter-terrorism and anti-terrorism preparedness measures.

actual impact or potential. Too often deterrence has been limited to expressions of reducing the incidence of violence, yet it is also about reducing consequences and bridging gaps in understanding. This apparent pragmatism in the concept of deterrence too easily dismisses or circumscribes considerations of mitigation, yet the reality is that a risk averse strategy is unsustainable because it is not commensurate with the actual risk and still cannot provide the certainties required, or indeed expected, in neutralising any threat.

Throughout the analysis of the controls and regulation of non-state micro-proliferation and use of CBR WMD capabilities, three central themes have evolved. The first is derived from the redundancies and pretence evident throughout the extant controls, where the predominance of effort is directed at export regulation and barrier controls, with a largely vacuous environment existing outside of these processes. Second is the premise that efforts are nearly entirely directed at those events after the fact, with little attention given to preemptive measures. Third, and most critical, the lack of uniformity and consensus vitiates aspects of enforcement, reduction, detection and responsiveness. It is as a consequence of these limitations that the capacity to estimate, and subsequently calibrate risk, is diminished and national regulatory structures exist wholly within a risk taking environment.

Antecedents that have previously underpinned the application of deterrence theory as a model to inhibit conflict between states are now increasingly being shaped within the parameters of an asymmetric threat landscape. As a precept, however, it must continue moving forward to considerations of suppression and neutralisation if deterrence as a theory is to maintain any relevancy. The Australian regulatory framework and its relative lack of effectiveness in countering micro-proliferation and the use of CBR capabilities by non-state actors will ultimately only ever be measured in outcomes. Yet the capacity to understand and establish counter-measures, and thereby manage aspects of the risk, cannot be found within a single range of measures or legislative instrument. Rather, the capability to develop a national deterrence strategy of any value, and in the process manage risk, is founded in the background clutter that is

commerce and research and the legislative framework that is more often the precursor to an event's occurrence.

Regulatory controls applied throughout the spectrum of risk materials, equipment and services will influence non-state outcomes. However, to the determined non-state organisation the prospect of halting all development, micro-proliferation or use, remains improbable. The internal and external influences on non-state organisations within a strengthened CBR regulatory environment have the potential to significantly inhibit or actually change outcomes, targets, operations, activities and capabilities. One of the better examples that illustrates this is to be found in the inadvertent, yet significant, exercise of deterrence through the regulation of hazardous substances, which in the end, positively influenced Ramzi Yousef's early attempts to develop a chemical and radiological capability which he had intended would be used in the 1993 World Trade Centre bombing.[99] Yousef attempted to increase the brissance and effect of the bomb he constructed through the use of additional hydrogen cylinders and radioisotopes. High costs, acquisition difficulties, transshipment controls and the increased likelihood of interdiction, clearly contributed towards influencing the cost-benefit analysis in Yousef's selection of delivery system, the construction of a device, and ultimately, in defining the bomb's limited effectiveness.[100] Hence, while largely inadvertent, what appeared as minor regulatory processes exerted a cumulative influence throughout the development process, eventually coalescing to alter the behaviour and capability development outcomes cycle of the group.

Controls are ultimately limited by what is to be regulated, the utility of the language used to define the requirement and how they are to be applied. Issues of compliance, enforcement and application, are in essence only as good as the framework and context against which they are set. The ad hoc structure

---

[99] Reeve, op. cit., pp 6-44.

[100] While there were many contributing factors, one of the more significant was clearly the ineffective placement of the vehicle and the underestimation by Yousef in the type and method of construction in the buildings, which was unlike the concrete reinforcement utilised throughout many other high risk buildings. The vehicle was not placed correctly against the inner core of steel support columns and it was assessed that even with effective placement, the desired outcome, that is, to topple both World Trade Centre towers, would have been unlikely. Reeve, op. cit., pp 6, 20-25.

throughout the existing range of controls, both in their seemingly haphazard development and limited enforcement, provide for only the perception of an effective national security framework. The national capacity and ability to positively influence change in non-state activities is largely diminished through a lack of an adequate judicial organ, emphasis on the act of use rather than on aspects of development, and a fundamental failing to look beyond the existing criminal justice framework to provide for greater reform.

Claims by states of increased regulatory controls, greater profiling and enhanced intelligence capacities following a terrorist incident, do little in contributing towards the application of any analytical rigor and attempts to develop strengthened deterrence strategies. The use of spurious documentation, illegal and covert acquisition, and activities which circumscribe regulatory structures, will likely be a continuing theme throughout most controls. The key in countering the increasing threat and impact from CBR capability development activities is not merely to be found in more capable response forces and sophisticated detection capabilities, but throughout the micro-regulatory controls that define every day trade and research. In the end it is the sale of a high risk chemical to an unknown purchaser, the uncertainty in the end-use and bona-fides of a request for the use of a scheduled poison, the lack of control and security of key precursors stored as dangerous goods, and other factors similar to these, that will define the efficacy of the CBR deterrence structures.

The national capacity to manage risk and a lack of understanding in its qualitative nature sees it perceived and applied as a process, rather than as a part of a wider strategy. It is applied through prescriptive solutions and mechanical practices, rather than as an element of a wider more insightful preemptive and deterrent process. Security is often applied under the pretence of risk management, but is more often constrained to measures akin to strategies of risk aversion or risk taking, eschewing those more critical considerations throughout the deterrence process – involving reduction, detection, enforcement and response to any threats. Establishing the level of risk is about understanding what it is that is unknown. There is no panacea or easily applied solution to minimise risks from non-state actions – conventional or unconventional. Yet the

uncertainty, indeterminateness and voids in understanding and knowledge throughout the non-state threat spectrum, rather than what is known, will be the more accurate measure in the efficacy of a states' response to these threats – 'we can never be certain; we are always ignorant to some degree'.[101]

The capacity to preempt micro-proliferation and the use of WMD capabilities is then dependent on the ability of the state to disrupt illegal and covert activities through the articulation of risk management throughout any counter-measures. While the act itself, such as the procurement of a key precursor or an item of biological equipment, may be entirely legitimate, recognising the potential and its likely end-use is at the crux of how non-proliferation, counter-proliferation and anti-terrorism measures are to be applied. As was declared in the introduction, this thesis can only ever provide the first step in any process of remediation. Society's cure for these threats can sometimes be as virulent a poison as the disease itself, particularly if misapplied or misunderstood. The complexity in the application of risk strategies and in attempting to effectively deter the prospect of any non-state threat, can be compared to a view through a kaleidoscope, where different patterns, assemblages and facets present themselves to the viewer. Yet the view is always different, dependent on the angle.[102]

The focus throughout the national spectrum of regulatory structures highlights a clear emphasis on human, animal and plant protection. International measures, while apparently appropriate in being applied to non-state actions and aspects of micro-proliferation of CBR capabilities, remain largely irrelevant. Paradoxically, it is then these same national and international regulatory safeguards that are relied on to provide measures of security and a preemptive capacity against the non-state threat, yet they largely maintain no deterrence value. This thesis has sought to highlight not just the vulnerability and pretence throughout many of these security structures, but to also place the theory and

---

[101] Bernstein, op. cit., p 207.

[102] J. D. Reisz, *A Theory on Terrorist Activity in America and its Effect on the United States Army*, Fort Leavenworth, Kansas, Masters Thesis, United States Army Command and Staff College, 8 June 1979, p 2.

management of risk in a context against which these increasingly lethal and more sophisticated technological threats may be mitigated. The permutations and combinations in how this can be addressed are many and one solution does not fit all. While the thesis has reaffirmed the need throughout policy, regulation and legislation for consistency, uniformity and specificity, counter-measures cannot be built around today's, or even tomorrow's, threat. The capacity to change, adapt and maintain a flexibility throughout any counter-measures, will in itself be the strongest deterrent.

Following the attacks in the United States on 11 September 2001, the national and international security, political and social environment is one of increasing aversion towards risk in the race to attribute blame and develop the evidentiary processes to establish a clearer cause and understanding of effect. There remains a real danger, however, in not recognising how much information is enough and how much is too much. The proclivity towards excessive attention to low-probability events accompanied by high drama, and the associated likelihood to overlook events that occur as routine or background, breaks down the processes for rational and deductive analysis. As with all disasters, follow up actions begin with purely rational decisions and analysis in managing risks which then move towards the extrapolation of what is, more often than not, just a run of luck.

> We put thirty spokes together and call it a wheel;
> But it is on the space where there is nothing that the
> utility of the wheel depends.
> We turn clay to make a vessel;
> But it is on the space where there is nothing that the
> utility of the vessel depends.
> We pierce doors and windows to make a house;
> And it is on these spaces where there is nothing that
> the utility of the house depends.

Therefore, just as we take advantage of what is, we should recognise the utility of what is not. Lao Tze, (Fourth century BC).[103]

[103] J. L. Everard, *Arms Control Discourse: The Salt Standing Consultative Commission 1975-1985*, PhD thesis, Australian National University, Canberra, January 1992.