The Information Component of National Power and Australian National Security Policy

Captain Jeff Malone *

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

*The views contained in this paper are the author’s own, and should not be construed as representing the views of the Australian Government or the Australian Department of Defence. The paper is unclassified in its entirety, and has been cleared for public release.

ABSTRACT

The paper critically surveys the role of the information component of national power (ICNP) in Australian national security policy. The paper commences with a review of the post-Cold War global security environment and the implications of the Information Revolution for national security. Following this, the paper proposes a model of the ICNP which operationalises the ICNP in terms of five inter-dependent national tasks. The paper then examines the Australian national security system and provides an initial assessment of its effectiveness at employing the ICNP. The paper concludes with a discussion of how the Australian national security system might be reformed so as to enhance employment of the ICNP in support of Australia’s national security objectives.

Keywords: Australia, information component of national power, national security

INTRODUCTION – NATIONAL SECURITY IN THE CONTEMPORARY ERA

In the wake of the Cold War, there has been a general recognition of the expansion of national security issues beyond traditional military, political and economic considerations. There had always been at least some acknowledgment of these other aspects of national security. But they tended to be sidelined in the militarily-defined bipolar world order in which the state was the pre-eminent organisational unit. So it is not unsurprising that when the Cold War world order collapsed in 1991, that the non-military aspects of security would immediately assume a new prominence. This has increased the complexity of national security affairs for two key reasons. First, the security agenda has broadened from focusing narrowly on military threats to consider a much wider range of issues. These have included climate change, uncontrolled population movements, trans-national organised crime, amongst a host of others. Second, the frame of reference of national security affairs has expanded from concentrating largely on the actions of states, to include a much richer consideration of the role played by non-state actors in the global security environment. So whilst states today are faced with a global security environment that is less overtly dangerous than during the Cold War, it is at once also one that is more challenging than was previously the case.

A ubiquitous feature of the emerging global security environment is the impact of the Information Revolution. The Information Revolution has fundamentally transformed economies and societies, and has yielded new bases for wealth, military power and political influence. But at the same time, the Information Revolution has eroded the ability of states to control information flows and has created new opportunities and vulnerabilities in critical infrastructures to external interference and disruption. Indeed, in global security terms, perhaps the key result of the Information Revolution has been to increase the reach and power of non-state actors with respect to states (Arquilla & Ronfeldt 1996: 133-134). But this should not be taken to herald the imminent demise of the state as a mode of organisation (Marsh 1996). Rather, in order for states to compete and prevail in the new global security environment, they must strive to understand the relationship between information and power, which is to say the information component of national power (ICNP) (Arquilla & Ronfeldt 1996: 134).
OPERATIONALISING THE INFORMATION COMPONENT OF NATIONAL POWER

Information-related activities have been present at the heart of strategy and statecraft since the dawn of human civilisation (ibid.: 132-133; Keuhl 1999: 3-4). But it is by virtue of the effects of the Information Revolution that the ICNP is now of unprecedented importance. Keuhl has offered the following formal definition of the ICNP:

‘The use of information, information processes and information tools as strategic instruments for shaping fundamental political, economic, military and cultural forces on a long-term basis to affect the behaviour of governments, supra-national organisations, non-state actors and entire societies to support national security objectives.’ (Keuhl 2000: 275)

The definition, though long, is useful on several accounts. It is technologically neutral, though in being so it is in no way incompatible with recognising the fundamental changes wrought by the Information Revolution. It identifies a variety of modes in which information impinges upon national security affairs: as a tool or weapon, as a target, or as a contested strategic resource. The definition notes that information-based tools and activities can impact across the different functional dimensions of national security. Finally, this approach to the ICNP recognises the complexity of the global security environment, by acknowledging the wide diversity of actor types on the world stage.

But defining the ICNP, whilst important, is insufficient. Rather, there is a need to operationalise such a definition: to translate the concept of the ICNP into tangible outcomes that might be implemented, measured and assessed. Following Dearth (Dearth 2000: 101-103), I propose that the ICNP can be understood in terms of the following five national tasks:

- **Intelligence** – the Intelligence task is the sum of all activities undertaken to collect and analyse information about the global security environment (and the actors within it) and to disseminate that processed information (intelligence products) to national security decision makers and executive bodies to support the achievement of national security objectives.

- **Counterintelligence** – the Counterintelligence (CI) task is made up of those active and passive measures taken to counter the intelligence activities of other global actors directed at ourselves.

- **National Information Infrastructure Protection** – the National Information Infrastructure (NII) protection task constitutes those measures taken to protect the NII from all sorts of hazards and threats (natural, accidental and deliberate) and different means (material, electronic and malicious or adverse computer code). NII protection is particularly challenging, both because it is largely owned by the private sector, and because of its seamless connection to the broader global information infrastructure (GII).

- **Perception Management** – the Perception Management (PM) task involves the conveying of messages to other actors in the global security environment, with the intention of influencing their behaviour and thereby achieving national security objectives. It comprises such activities as Public Diplomacy (PD), International Public Information (IPI), and (controversially) deception and covert information dissemination activities. PM is a routine part of the overall conduct of statecraft, but it takes on an enhanced urgency during times of crisis and conflict.

- **Information Operations** - The use of military means to shape the global information environment in support of national security objectives. Whilst Information Operations (IO) has both offensive and defensive components, it is principally through the employment of offensive capabilities (such as electronic attack and the physical targeting of information infrastructure) and overall force posturing that IO contributes towards the ICNP.
These five tasks should not be seen as stand-alone pillars – rather they are all heavily inter-related, though not necessarily each to the same extent or in the same way. The five tasks do not align neatly with traditionally established government departments and agencies. Rather, each of these functions will cut across boundaries between different national departments and agencies, different levels of government, and across the public/private divide. Each of these five tasks are also closely linked to a range of other national security issues. Intelligence, CI and PM are the stock-in-trade of statecraft and touch upon virtually every aspect of national security policy. NII protection is intimately related to the broader issue of the protection of other elements of critical national infrastructure (CNI) such as water and power supply, transportation networks, the financial system and so forth. IO cannot be readily disentangled from the overall conduct of military operations in support of national security objectives. And the ICNP as a whole is closely associated with broader national policies relating to the collection, transport, storage and use of information in all its forms. Hence, the ICNP cannot be understood in isolation from these other policies, which in aggregate might be held to constitute a national information policy (NIP).

THE AUSTRALIAN NATIONAL SECURITY SYSTEM

Having provided a conceptual account of the information component of national power, attention will now be focused the mechanisms by which this might be employed in an Australian context: the Australian national security system. As the result of historical influence of the UK, the Australian national security system is characterised by a relative lack of formal organisational structures and processes. Until recently (May 2003), Australia has never established a focal body comparable to the US National Security Committee (NSC) staff (which was set up in 1947 essentially to deal with the unfolding Cold War) to deal with national security issues on a full-time basis (Oatley 2000: 11).

Similarly, no Australian government has ever formally articulated a comprehensive national security policy (ibid.: 6). Rather, the core of Australia’s national security system has been a series of part-time committees that meet on an ‘as-required’ basis (ibid.: 10-14). Reflecting the essential informality of the Australian national security system, literature dealing with formal organisation and process in Australian national security policy is sparse. Key works are Swinsburg 2001, Oatley 2000, Brown 1994 and Ball 1982. The outline structure of the Australian national security system is shown below as Figure 1.
The apex of the Australian national security system is the National Security Committee of Cabinet (NSC). NSC is a Cabinet sub-committee comprised of the Prime Minister (Chairperson), the Deputy Prime Minister, the Treasurer, the Minister for Foreign Affairs and Trade, the Minister for Defence, the Attorney-General and the Minister for Immigration and Multicultural and Indigenous Affairs. Other Ministers are seconded to the committee when specific issues relevant to their portfolios are being addressed (National Security 2003). Supporting the NSC is the Secretaries’ Committee on National Security (SCNS), which is comprised of the public service heads of the departments noted above. It also includes the Chief of the Defence Force (CDF) as the principle military advisor to government and the Director-General of the Office of National Assessments (ONA) as the principle intelligence advisor to government (Oatley 2000: 25). Both NSC and SCNS are supported by a third, less formal, body – the Strategic Policy Coordination Group (SPCG). The SPCG is staffed at the Deputy Secretary/Vice Chief of the Defence Force (VCDF) level (ibid.: 26). A small staff resident in DPMC provides secretariat support for these three bodies.

Below these senior committees, there is on the one hand the individual departments and agencies involved in the delivery of national security outcomes, and on the other hand, a range of inter-departmental and inter-governmental committees and task forces. These can either be permanent (standing), or created for a limited duration for a specific purpose. The arrangements include the Australian Intelligence Community (AIC), inter-departmental arrangements (comprising solely of federal departments and agencies) and inter-governmental arrangements (including departments and agencies from both the federal and state levels of government). The last of these reflects the considerable powers that reside at the state, rather than federal level of government in Australia, particularly as regards counter-terrorism and coastal surveillance and protection.

A key feature of the Australian national security system is that mechanisms for coordinating whole-of-government and inter-agency outcomes have traditionally been, and remain, relatively weak. In the wake of the 11 September 2001 attacks and the 12 October 2002 Bali bombing there has been a flurry of activity in the policy departments and agencies, and some modifications in the coordinating mechanisms for dealing with counter-terrorism (NCTC 2002) and NII protection (Williams & Alston 2002). But the core functioning of the Australian national security system has remained essentially unchanged. Announcements in May 2003 regarding the creation of a new National Security Division (NSD) within DPMC may indicate a move toward the creation of stronger organisational mechanisms for developing and coordinating national security policy (Shergold 2003). But as these arrangements have only been in place since July 2003, it is as yet too early to assess their potential impact. Further, the newly appointed head of NSD is on the public record as stating that he saw no requirement in Australia to promulgate a formally articulated national security policy along the lines of the US National Security Strategy (Jordana 2003).

THE PLACE OF THE INFORMATION COMPONENT OF NATIONAL POWER IN THE AUSTRALIAN NATIONAL SECURITY SYSTEM

The preceding section provided a high level overview of the structure and operation of the Australian national security system. In this section, attention will be focused on how the Australian national security system employs the information component of national power. Before proceeding, it should be noted that just as Australia has no formally articulated national security policy, no Australian government has ever formally articulated the place of the ICNP as an element of national security policy. Indeed, no Australian government has ever articulated a formal NIP (Willingham 1998), but elements of what might collectively constitute a NIP have over the years been embodied in various pieces of policy and legislation (Middleton 1997: 10). Over the last two decades there have been a number of attempts at articulating a NIP proper for Australia (both within and outside of government) (DOS 1985; Judge 1985; HRSTCFLTS 1991; CRC 2001). But none of these have received official sanction, and in any case they have touched but lightly on national security matters, if at all.
But this is not to say that elements of the ICNP are not formally recognised in the Australian national security system. Within the AIC, organisations and arrangements are in place to perform the national intelligence and CI tasks (Andrew 1992: 82-114; Gyngell & Wesley 2003: 133-160). In the PM arena, Australia has long undertaken a range of international broadcasting and public diplomacy activities to create a positive image of Australia (Hodge 1995: 226-278; DFAT 2003: 129-130). More recently, a range of mechanisms have emerged for the protection of the NII (NOIE 2001; Williams & Alston 2002). And the ADF has adopted the concept of IO, and is enhancing its ability to conduct IO as an integral part of its overall repertoire of missions (Malone 2003). So the ICNP is not absent from the Australian national security system. Rather, it is present in a piecemeal, disaggregated fashion.

Noting the above, how effective has Australia been in employing the ICNP in support of its national security objectives? A detailed examination is beyond the scope of this paper, but an initial survey is not promising. In the case of the intelligence function, concerns have been expressed that the intelligence assessments and reporting process has been deformed by imperatives arising out of the electronic media cycle rather than the demands of national security (Woodard 2001: 20; Sheridan 2002; Nicholson 2003). In terms of the CI function, there has been a narrow focus on the protection of classified government information and the CI system has failed to address the issue of espionage directed at Australian commercial or other private interests (Dempsey 1999; O’Neill 2001). In terms of NII protection, it has been argued that the present arrangements are under-funded, poorly coordinated, and have been ineffective in engaging the private sector (Gamertsfelder 2002: 10; Dearne 2002; Riley 2003; Dearne 2003a). In the case of the PM function, there are no effective standing arrangements for coordinating government messages directed at foreign audiences. Further, PD and international broadcasting have been poorly resourced, and have suffered financial cut-backs as the result of domestically-driven political agendas (Editorial 2001: 14; SFADTRC 1997: 153-156). And whilst the ADF has been fairly successful in employing IO at the tactical and operational levels of organisation, these have not been supported at the strategic/national level (ANAO 2001: 110-111; Beasley 2002: 21-22). In short, an initial assessment of Australia’s ability to employ the ICNP that it does so poorly.

Why is this the case? There would appear to be four key reasons for this. The first is the absence in Australia of a national security policy document that articulates the full scope of Australia’s national security objectives, and the place of the various instruments of national power in achieving those objectives. Such a document might provide the broader framework within which the employment of the ICNP could occur. In the absence of such a framework, it follows that it is correspondingly difficult to articulate what role the ICNP might play. The second reason is that the role of the ICNP in achieving national security objectives has never been formally considered in Australia. As the result, programs or activities that might conceivably contribute toward the ICNP (and therefore the achievement of national security objectives) have often been sidelined by domestic political imperatives. In defence of Australia’s situation, no other state is known to have clearly articulated the role of the ICNP within its overall national security policy. Arguably, the United States has come closest to doing so in the various iterations of its publicly released National Security Strategy documents (Kuehl 2000: 272-287). But even so, the most recent version of this document (released by the G.W. Bush administration in September 2002) (Whitehouse 2002) has been perceived as a retrograde step (Kuehl 2003).

The third reason for the poor employment of the ICNP within Australia is the weak state of integrating mechanisms within the Australian national security system. As was noted previously, the constituent elements of the ICNP are spread across different national departments and agencies, different levels of government, and in both the public and private sectors. Accordingly, the effective employment of the ICNP (whether formally acknowledged or not) is critically dependent upon coordinating mechanisms that must bridge the inter-departmental, inter-governmental and public-private divides. It is just such integrative mechanisms that are generally lacking in the present Australian national security system, built as it is upon part-time and ad-hoc committees. And the fourth reason, which underscores the above three, is the poor level of understanding of the ICNP of national security decision makers,
particularly at the senior level. It is scarcely surprising that the ICNP is poorly represented in Australian national security policy: those responsible for wielding it are largely ignorant of it and the implications of the Information Revolution for national security affairs.

ENHANCING THE INFORMATION COMPONENT OF NATIONAL POWER IN THE AUSTRALIAN NATIONAL SECURITY SYSTEM

Given the above negative assessment, how might Australia’s ability to employ the ICNP be enhanced? Possible solutions resolve into two sets of proposals: those that address the issue of the ICNP as a whole; and those which address specific shortcomings noted in the five national tasks. In terms of the ICNP as a whole, action should start with the drafting and publication of a proper national security policy, which encompasses all the dimensions and instruments of national power. As has been noted previously, such a national security policy document would provide the framework within which the ICNP sits. But there are further benefits to such a document. It can communicate strategic vision to a range of audiences, both internal and external (Kuehl 2000: 276). Accordingly, such a document can encourage greater public awareness of national security issues (Oatley 2000: 21) as well as contributing towards the national PM task (Kuehl 2000: 276). Finally, the very process of drafting such a document can contribute toward the consensus and integrative arrangements that a comprehensive national security policy requires in order to be implemented (ibid.).

Second, there is the need to recognise the ICNP within overall national security policy. Whilst this could take a variety of forms, Keuhl’s definition and the five national tasks described above represents a workable approach. The formal recognition of the ICNP would serve two main tasks. It would provide the framework within which more focused reforms of specific elements of the ICNP (described below) might occur. And it could also serve an educational purpose, by increasing the awareness and understanding of the ICNP in decision makers and their supporting staffs in the Australian national security system. Third, there is a need to strengthen the integrative mechanisms in the Australian national security system, by augmenting the present system of part-time committees with a full-time staff dealing with national security matters. There are indications that such reforms are already under way, in the form of the new NSD within DPMC (Shergold 2003). But creating effective integrative mechanisms might ultimately require a fully-fledged national security body, along the lines of the US NSC staff (Oatley 2000: 21).

In terms of addressing shortcomings in the five national tasks within the ICNP noted above, the following proposals might be considered:

- **Intelligence** – There is need for greater level of professionalism in the AIC, particularly as regards strategic assessments and overall management of the intelligence process (ADA 2003). This would help insulate both the intelligence analysis and dissemination activities from the more pernicious effects of the global electronic media, and the imperatives that it induces in the political system.

- **CI** – The CI system needs to broaden its conceptual horizon to consider the national security ramifications of information held outside of the public domain. This would not necessarily require legislative action as elaborate the US 1996 Economic Espionage Act (Bellocci 2001). But at the very least this would require an expanded definition of espionage, as compared to the one that presently exists in Australian legislation.

- **NII Protection** – There is a need to consolidate the present NII protection arrangements, and to provide greater incentives for private sector involvement in NII protection through both incident reporting and the efforts it takes to protect itself. A possible model for more integrated NII protection measures is the UK National Infrastructure Security Co-ordination Centre (NISCC), which brings together the various UK government NII protection stakeholders (NISCC 2002). On the later issue, tax breaks for corporate spending on protecting privately owned parts of the NII have been proposed as a means both for creating an incentive for private sector action, as well as socialising the cost of enhancing the security of the privately owned components of the NII (Dearne 2003b; Gamertsfelder 2003).

- **PM** – There is a need to establish standing arrangements for the coordination of messages directed at foreign audiences, analogous to the US government’s Office of Global Communications (OGC) (Whitehouse 2003) or the UK government arrangements (Rowlands 2003). Further, consideration should be given to reforming the funding and governance arrangements for Australia’s international broadcasting activities, so that decisions on these matters are not driven solely by domestic political considerations. Models for this exist in the US, UK, Canada and elsewhere (SFADTRC 1997: 113-114; 208).
IO – There is a need to continue enhancing the ADF’s IO capabilities at the tactical and operational levels, and to improve significantly the strategic integration arrangements both across the entire DOD, and between the DOD and other national departments and agencies. A possible model for this is the Directorate of Targeting and Information Operations (DTIO) in the UK Ministry of Defence (MOD). DTIO was set up as the result of the poor showing of UK and allied IO during Operation ALLIED FORCE in Kosovo in 1999 (HOCDC 2001, para. 67). DTIO acts as the proponent for IO within MOD, and provides a focus for integrating MOD IO activities with the broader UK government employment of the ICNP (Smith 2003).

The above proposals all have resource implications, potentially quite significant ones, though these are difficult to quantify immediately. That said, measures to overall the national security system as a whole will also have a direct impact on the effectiveness of these five national tasks. But ultimately, decisions about enhancing the ICNP must revolve around both the effectiveness of the national security system, not only its ‘efficiency’ in a narrow financial sense (Oatley 2000: 21). If the national security system is incapable of effectively employing the ICNP, or wielding other instruments of national power, then its supposed ‘efficiency’ will count for naught.

CONCLUSION

Information and information-based activities have been an integral part of statecraft and strategy since the dawn of human civilisation. But a key outcome of the presently unfolding Information Revolution is that the prominence of information as a tool/weapon, target and strategic resource has increased to a level hitherto unknown in human history. Accordingly, the ICNP is of increasing importance in the emerging global security environment. In turn, it follows that the ICNP is of vital significance for the conduct of Australian national security affairs. This would appear to be the case on two accounts.

Harnessing the ICNP is vital for Australia as a prospective Information Age state, economy and society. Australia, in common with other Information Age states, is critically dependent upon the evolving GII. On the one hand, the hyper-connectivity provided by the GII is a potential source of wealth, power and influence. But at the same time, such dependency creates vulnerability to influence and attack by others, particularly by actors that previously could not hope to challenge states. Reconciling the potential benefits with the risks to the nation created by hyper-connectivity is no easy or clear task. However some guidance on such matters might be provided by formal recognition of the ICNP and its place within an overall national security policy.

But in an Australian context, there is further significance to the ICNP. In world terms Australia is a fairly small state with only modest resources to influence and shape the global security environment. Further, this needs to be understood against the backdrop of an increasingly unstable and insecure regional and global security environment in which Australia’s interests and values will be increasingly challenged and threatened (Reilly 2000; DFAT 2003: 16-19; DOD 2003: 8-22). But Australia has the potential – by intelligently employing informational means – to wield influence well out of proportion to its size. Indeed, the ICNP may well prove to be the most important means for Australia to achieve its national security objectives. So harnessing the ICNP is vitally important for Australia’s present and future national security. It is something that is downplayed or ignored at Australia’s peril.

ABBREVIATIONS AND ACRONYMS

ADA – Australian Defence Association (Australia)
ADF – Australian Defence Force (Australia)
AGD – Attorney General’s Department (Australia)
AIC – Australian Intelligence Community (Australia)
ANAO – Australian National Audit Office (Australia)
CI – counterintelligence
CNI – critical national infrastructure
CRC – Chifley Research Centre (Australia)
DFAT – Department of Foreign Affairs and Trade (Australia)
DOD – Department of Defence (Australia)
DOS – Department of Science (Australia)
DMPC – Department of Prime Minister and Cabinet (Australia)
DTIO – Directorate of Targeting and Information Operations (UK)
GII – global information infrastructure
HOC – House of Commons (UK)
HRSTCLTS – House of Representatives Standing Committee for Long Term Strategies (Australia)
IDC – inter-departmental committee
IO – Information Operations
MOD – Ministry of Defence (UK)
NCTC – National Counter-Terrorism Committee (Australia)
NII – national information infrastructure
NISCC – National Infrastructure Security Co-ordination Centre (UK)
NOIE – National Office of the Information Economy (Australia)
NSC – National Security Committee (US)
NSCC – National Security Committee of Cabinet (Australia)
NSD – National Security Division (of DPMC) (Australia)
OGC – Office of Global Communications (US)
ONA – Office of National Assessments (Australia)
PD – public diplomacy
PM – perception management
SCNS – Secretaries’ Committee on National Security (Australia)
SFADTRC – Senate Foreign Affairs, Defence and Trade References Committee (Australia)
SPCG – Strategic Policy Coordination Group (Australia)

REFERENCES


NCTC (2002) – Communique of the 13-15 November 2002 meeting of the National Counter-Terrorism Committee, Canberra, November. HTML document available from:
Jeff Malone


