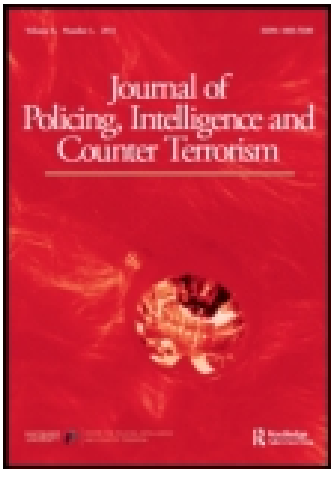

Journal of Policing, Intelligence and Counter Terrorism
Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/rpic20

Intelligence Informatics … Transforming the Australian Intelligence Community

Kevin Monks [a]
[a] School of International Studies , University of South Australia
Published online: 03 Aug 2011.

To cite this article: Kevin Monks (2008) Intelligence Informatics … Transforming the Australian Intelligence Community, Journal of Policing, Intelligence and Counter Terrorism, 3:2, 62-87, DOI: 10.1080/18335300.2008.9686914

To link to this article: http://dx.doi.org/10.1080/18335300.2008.9686914

Intelligence Informatics … Transforming the Australian Intelligence Community

KEVIN MONKS
School of International Studies. University of South Australia

ABSTRACT

Australia is challenged with providing timely and accurate intelligence to decision-makers amidst a dynamic global environment. People and products move constantly across country and regional boundaries, requiring increased sharing and coordination of information between domestic and international agencies. Information technology and communications advancement multiplies the complexity by creating information overload for the intelligence analyst and information architect.

While the 2004 Flood Inquiry made several sensible and safe recommendations across the intelligence community, their report, and in all fairness their remit, fell short of addressing the best way to organise and equip the AIC given the emergent threats to Australia, the inefficiencies of intelligence collection and production, the lack of performance metrics and feedback, and the absence of cross-community management tools. Although Australia's determination to bolster national security has manifested itself in different forms, important structural and cross-community issues have yet to be fully addressed. This paper recommends further constituent changes to improve the way in which the AIC collaborates and manages organisational knowledge.

The Australia Intelligence Community (AIC) is challenged with providing timely and accurate intelligence to decision-makers amidst a dynamic global environment. People and products move constantly across country and regional boundaries, requiring increased sharing and coordination of information between domestic and international agencies. Websphere and communications advancement multiplies the complexity by creating information overload for the intelligence analyst and information architect.

While continuing to recognise the importance of longstanding security relationships, the Australian consciousness is transitioning toward an increasingly multilateral perspective as a resident of the Asia-Pacific region and as a "middle-state" global intermediary. Australia has invigorated environmental issues such as the Kyoto Protocol on greenhouse gases and is attempting to re-energize nuclear non-proliferation and disarmament (Rudd, 2008). Australia is a dialogue partner within the ASEAN (Association of Southeast Asian Nations) Regional Forum and is a signatory to a large number of international agreements and treaties, many under

United Nations sponsorship. Economic engagement with regional industrial giants, India and China, has re-focused the bore sight, primarily due to the expansion of trade and a vibrant resource sector. Coupled with the volatile Western marketplace as well as the costly and questionable excursions in the Middle East and Afghanistan, Australian sentiment appears to be shifting toward a new public perspective.

With all this change, the culture of the AIC has not significantly transformed in the last fifty years. In an increasingly bureaucratic and legalistic business environment, there is a propensity toward each ascendant layer diluting assessment through the addition of qualifiers and disclaimers. Conversely, the provision of good intelligence assessment from the AIC does not necessarily guarantee good policy and decision-making by leadership. An effective intelligence community will, however, bring to light emerging threats and indicate ill-advised policies and plans are unfeasible (Chesterman, 2006).

While the Report of the Inquiry into the Australian Intelligence Agencies (Flood, 2004) made several sensible and "safe" recommendations across the intelligence community, their report, and in all fairness their remit, fell short of addressing some major issues. For instance, the Flood Report did not address the best way to organise and equip the AIC given the emergent threats to Australia, the inefficiencies of a fatigued intelligence structure, the lack of performance metrics and feedback, and the absence of cross-community management tools. The AIC continues to operate within organisational stovepipes based upon "intelligence-type" which somewhat limits transformational change to product dissemination and specific mission processing. Endeavours have made headway into data fusion (the integration of intelligence from different sources) and data sharing. However, this has primarily been a techno-centric response to defence and counter-terrorism customer requirements. Knowledge management from the organic organisational or ecological perspective has not been seriously addressed across the AIC.

Informatics is the science of information which studies the structure, behaviour, and interactions of systems that store, process and communicate information. Since computers, individuals and organisations all process information, intelligence informatics has computational, cognitive and social aspects that require investigation (Fourman, 2002). The field of knowledge management theory also applies to the study of the generation, representation, access to, and transfer of knowledge and can provide a foundation for further research into intelligence community design. Through the application of informatic and knowledge management principles, a new intelligence structure and process can emerge to better meet existing and future AIC challenges and, ultimately, increase the performance and accountability of the community and government.

There are multiple schools of thought regarding the need to improve the AIC (Cotton, 2006; Dudgeon, 2006; Flood, 2004; Gordon, 2005; James, 2004; Peppler, 2006; Wilkie, 2004). The views vary from implementing a comprehensive institutional overhaul, to increasing certain analytical tools and personnel expertise, to the belief that change will create more disturbance than net sum gain within the business of intelligence. Given the large amount of dynamic information and the trans-national

nature of the challenges confronting the AIC, it is evident that a dramatic increase of interaction between agencies and nations is required. Organisations, as well as countries, which historically were able to continue to operate in a relative vacuum must now cooperate with counterpart (and sometimes rival) organisations at the national, state, and local levels. The growth in multi-national response to international situations also requires Australia to collaborate with international police, investigative, and intelligence agencies.

A new structure

The requirement for interoperability within the AIC has grown significantly. As the Flood Inquiry points out, "new roles and increasing demands have brought about greater challenges in managing interfaces and new relationships" (Flood, 2004, p. 70). The current AIC organisation does not have sufficient connectivity, traceability or the system tools between producers and consumers of intelligence to ensure the provision of accurate and timely assessment. Existing structure also continues to rely heavily on a minimally staffed and policy-oriented ONA to digest large volumes of intelligence and present their assessment to leadership. This arrangement does not take full advantage of the multitude of cross-community expertise that could be harnessed within Australia (Gordon, 2005, pp. 54-57). The AIC structure must be appropriately configured and populated if it is to be responsive to an array of concurrent international and in-country demands. These circumstances are the core justification for a re-evaluation of the AIC architecture and associated processes.

In the business environment, companies want their activity to be and remain different than other businesses in order to maintain a competitive edge. While competitiveness can be seen to sharpen contestability within the AIC, competition, in general, can hinder an intelligence community's willingness to collaborate. A new AIC structure should be mindful of lessons learned from past and current intelligence community experiences, address challenges internal and external to the community, and seek to incorporate tenets of knowledge management and information sharing. A re-structure should be undertaken to arrange the AIC into a more functional organism which will allow the pre-existing elements to maintain, for the most part, their organisational integrity. This will be an important feature of any proposed new design as an unrecognisable, radical transformation will most likely be rejected due to the establishment's perception of unwarranted risk.

As a result of research into the published AIC structure, foreign intelligence community structures, intelligence professional commentaries, the Flood Report, and personal intelligence community experience and interpretation, I submit a potential structure for consideration (Figure 1) to further the investigative process. Responsibilities are enhanced, transferred, or centralised. New leadership positions are created (Director of Trans-national Intelligence and Director of Defence Intelligence), and two new entities are created (National Mission Management Centre and the Directorate of Information Access and Management). Structure and process

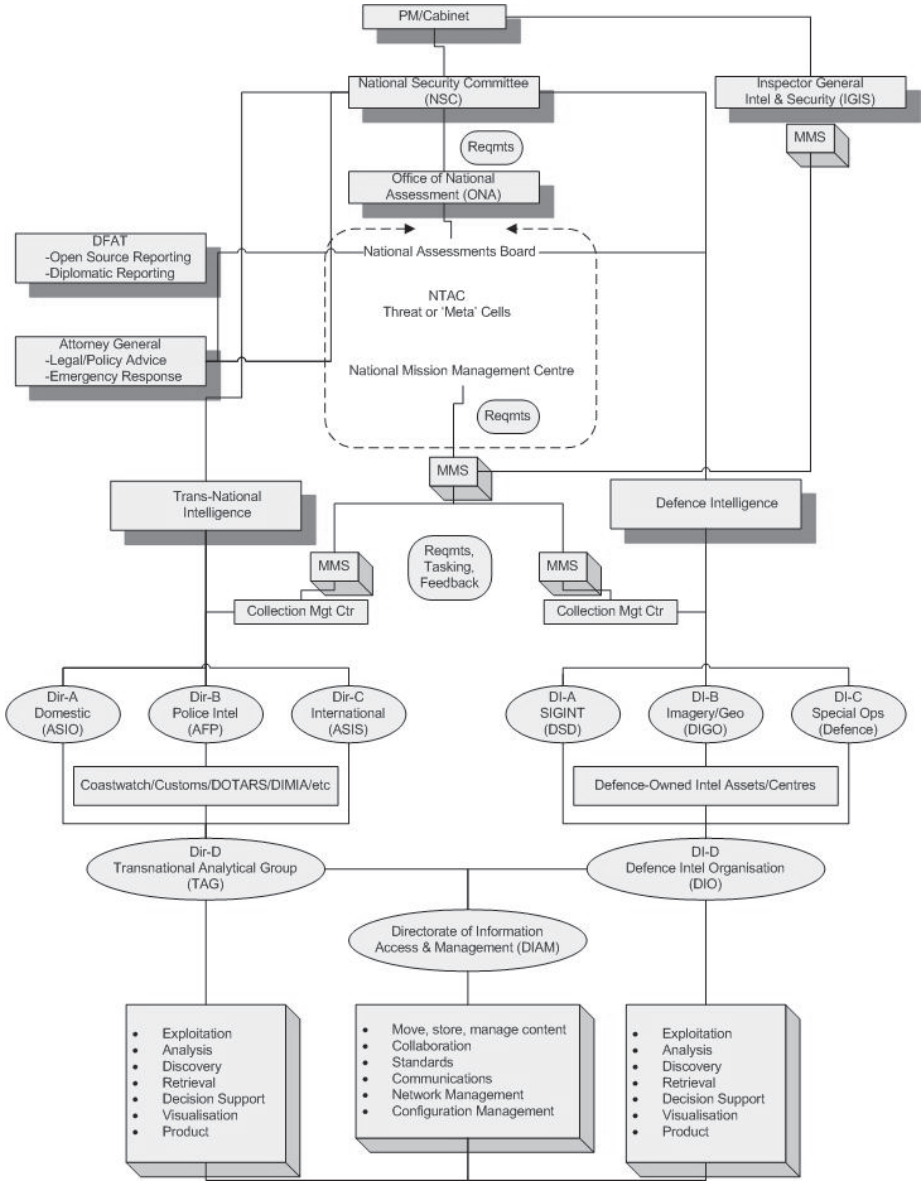

Figure 1 – Proposed future AIC structure

change can begin the transformation of the AIC environment. Designing a collection management and analytical core that can readily transform to meet new challenges, as a complex adaptive system, while maintaining a stable AIC organisational shell that can ensure accountability, traceability, and information sharing is critical if Australia is to prepare and respond intelligently in the future.

Organisational responsibilities and process

PRIME MINISTER AND NATIONAL SECURITY COMMITTEE OF CABINET

In the hypothetical architecture, the Prime Minister and National Security Committee of Cabinet (NSC) continue in their current roles as primary decision-making body and budget setter for national security, including foreign and domestic intelligence matters, and interact with the Secretaries Committee on National Security (SCoNS), and other related committees and council groups. The NSC continues to review and provide direction on intelligence priorities, resources, and staffing policies. The NSC, however, must step up their awareness of national priorities setting and adjustment due to the rapid rate of situational change injected by increased globalisation and economic inter-dependency (Oatley, 2000, pp. 13 & 25). The senior echelon should also attempt to keep the AIC aware of pending policy and decision issues that could potentially impact the associated national intelligence priorities managed by the Office of National Assessment (ONA). The process to gather the needs of senior decision makers across the Australian government should be accomplished on a regular basis to support prudent allocation of both collection and analytical resources.

The Flood Report rightly stated that "a strong priority setting mechanism is vital for a healthy intelligence system" (Flood, 2004, p. 66). Interpreted from the national intelligence priorities provided by the SCoNS for approval by NSC, the collection requirements issued by ONA should contain sufficient guidance detail to ensure that collection items are not being over-tasked. A classical gap in national guidance can be the issuance of a relatively vague collection priority list which is left for the collection management agencies to interpret which, in turn, may require a task to be collected on a 24/7 basis. It may not be feasible to attempt collection on a task due to limitations such as time of day access or a low probability of obtaining anything useful for other reasons. Some requirements are justified for continuous collection. This clarification should be included within the collection guidance. Collection resources can be freed up to be applied to other currently middle to lower priority tasks if the extra step in clarification or a further level of requirement analysis is applied. Middle to lower tasks (particularly in the new target development arena) have a tendency to suddenly rise to high priority tasks as the community experienced in the lead up to the first Gulf War. Having a modicum of information on a new area is better than having to start from scratch at the onset of a new hot spot or crisis support. This discussion should take place between SCoNS, ONA and the intelligence chiefs, be clarified in the national priority guidance, and reflected in the proposed National Mission Management Centre and Collection Management Centre tasking messages.

In the hypothetical structure, the PM and NSC will continue to utilise ONA for top-priority national assessments, will assign two new direct-reporting chiefs for trans-

national and defence intelligence matters, and will also have an enhanced Inspector General – Intelligence and Security (IGIS) capability to provide independent AIC-wide performance measurement and feedback.

OFFICE OF NATIONAL ASSESSMENT (ONA)

ONA, and its leader the Director-General, would have a greatly enhanced role in the new hypothetical architecture by assuming the responsibility for the new National Mission Management Centre (NMMC), the National Threat Assessment Centre (NTAC), and for accommodating the new Trans-National and Defence Intelligence interface. ONA would continue to be responsible for drafting National Assessments in consultation with other relevant agencies before they are considered by a National Assessments Board. The ONA strategic assessment activities would be stepped up to former productive levels on international political, strategic and economic developments. The National Assessments Board, which is chaired by the Director-General of ONA, would expand its representatives to include the new Trans-National and Defence Intelligence chiefs to provide intelligence source representation and verity as part of the process.

ONA – NTAC

The new ONA structure would incorporate the National Threat Assessment Centre (NTAC) which is currently located under the jurisdiction of the Attorney General. The NTAC, comprised of multiple agency representatives, is more appropriately positioned under the ONA as it is a national assessment group. Centralising national security assessment under the Australian Office of National Assessment is a sensible approach. The activities being tracked by the NTAC transcend Australian borders – organised crime, terrorism, money laundering, people smuggling, and a host of other threats. Moving the real-time tracking and coordination of the threat assessment centre under the same organisational umbrella as long-term strategic assessment would create a single "home" for assessment. It would also facilitate communications under the new structure, being co-located with the NMMC and the national assessment community.

The new NTAC would be comprised of Threat or Situation Assessment Cells (also referred to as "meta cells") which will be assigned the highest priority national intelligence missions. The NTAC scope would expand through the creation of community-wide assessment cells that are formed to address major national and international security situations (e.g. terrorism, organised crime, peace-keeping mission, or a country of interest). The NTAC Cells would be populated with community-wide analytic and collection discipline/system specialists seconded from Trans-National, Defence, or elsewhere in government or industry. The cell could be tailored to focus specific mission expertise on the particular situation. Cells could be duplicated on an exceptionally important topic if contestability is required. The ability to mix and match analytical skill sets according to the situation would accelerate greater coordination, networking, and cross-training among Australia's intelligence agencies (Flood, 2004, p. 107).

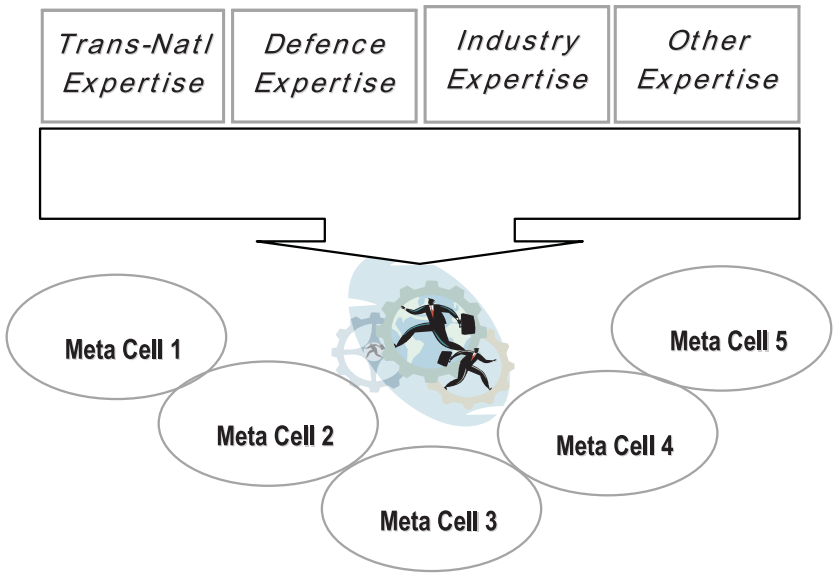

Figure 2 – ONA NTAC threat assessment or 'meta cell' concept

Each NTAC "meta cell" would own the responsibility for the Community's analysis on their respective issue as well as direct and receive all AIC product related to their issue. Routine, ongoing political, economic, and defence intelligence analysis would continue within the Trans-National Analytical Group (Dir-D in Figure 1) and in the Defence Intelligence Organisation (DI-D in Figure 1). Dir-D and DI-D would expedite and forward intelligence which relates to specific NTAC cell activity. Cells would be formed and disbanded per the direction of ONA and approval by the NSC.

The NTAC cell arrangement would also ensure that funding for high priority issues is appropriately prioritised and visible within the AIC budget and supports the Dir-Gen ONA, Trans-National Intelligence Chief, and Defence Intelligence Chief strategic direction for the AIC (Kinsvater, 2003). The new ONA NTAC would build on the current NTAC approach, would provide a collaborative, AIC-wide focus and mission set, and help to increase cooperation and teamwork. Under this new structure, ONA would become the heart of the Australian intelligence community, directing national mission management, housing active cross-organisation populated meta cells, and conducting traditional strategic assessment.

The NTAC cell teams should be encouraged to engage knowledge exploitation and knowledge management principles, sharing and growing relevant, timely intelligence assessment through the thorough analysis and provision of all-source product. This could include training intelligence professionals in areas such as network theory (networks are not random but have underlying structures and accompanying patterns) and Actors-Activities-Resources-Ideas modelling (AARI) (Welch & Wilkinson, 2000; Hakansson & Snehota, 1995; Hellgren, 1993). Community education could also include overviews of decision analysis, which can employ tools, methodologies and software to help people make better decisions (Poulton, 1994) and complexity

science, which studies systems with many parts that interact to produce global behaviour that cannot easily be explained in terms of interactions between the individual constituent elements (Waldrop, 1992; Perez et al., 2006). Information theory is used in information retrieval, intelligence gathering, and statistics. The communications engineer, systems analyst, and the information technologist are the agents within the AIC who primarily operate within the information theoretical realm. Even though aimed at the technical aspects of communication, it should be noted that the theoretical objectives of information communications and messaging also applies to the organisational and operational aspects within the AIC. Communications challenge the AIC on a daily basis, whether it is in the successful transmission of an intelligence task to a collector, an assessment to a customer, or the minimization of distortion to the "knowledge message".

Organisations embrace knowledge management if they believe that it will lead to greater innovation, business process consistency, better customer experiences and cross-organisational knowledge access (Dilnutt, 1999). Information and knowledge management, when properly thought out, can represent a major and beneficial opportunity for change. Conversely, Milner states:

> "Ill-considered and inadequately piloted change represents a threat of making things worse within the public service, perhaps even exacerbating exclusion" (Milner, 2000).

R. Lievesey-Howarth declared:

> "We can disenfranchise millions of people, and some say the ICT industry is doing just that … so much is changing. We must not think of computer-literate people but people-literate computers. The information society can be built around the citizens, rather than the current trend of government building infrastructure around itself … This is a community issue" (Lievesey-Howarth, 1997).

Over the collective history of the AIC, the sharing of knowledge has not been a community strongpoint. The way in which the independently operated units (stovepipes) have been formed and the onerous requirements to protect the information inherently defaults organisational behaviour to the side of isolation rather than an atmosphere of interoperability. The primary focus is on an individual organisation meeting an individual consumer's intelligence requirement. If information is required to be shared outside of that relationship, it must go through a number of wickets (security, political, technical, etc.) before the exchange can occur. The system and culture are not conducive to a knowledge community framework.

The challenges to the AIC will continue to be non-conforming. This will require the movement of blocks of knowledge and expertise together in combinations. All of the expertise required to meet the variety of intelligence challenges may not be located within the AIC organisation. There are many in Australia who have specialised technical, organisational, think tank, or regional-cultural skills that would not be available for a full-time AIC position but would be willing to periodically augment

the AIC when called upon to do so. A mechanism to tap into these resources, such as an intelligence reserve corps, would greatly benefit the AIC.

The NTAC cell team concept will be able to incorporate complex adaptive system principles and qualities, providing the AIC with a more flexible response to ever-changing challenges. This approach will also begin the community shift from an individual collection agency orientation to a more collaborative "intelligence issue-centred" culture.

Within this new architecture, it is proposed that the NTAC be placed within ONA and all other ASIO intelligence responsibilities be moved from the Attorney General's Office portfolio and be placed under the Trans-National Intelligence organisation. With the exception of the NTAC, the ASIO Director would retain all current responsibilities within the Trans-National Intelligence envelope. The NTAC, within ONA, would be ministerially responsible to the PM. The Attorney General would continue to be a member of the NSC of Cabinet.

ONA – NATIONAL MISSION MANAGEMENT CENTRE (NMMC)

There is an urgent call for a nationally responsible intelligence requirements and task management centre and system. There are currently a variety of centres, systems, nomenclatures, and procedures being used across the AIC organisations. The national intelligence requirements identification and prioritisation control (Gordon, 2005, p. 30) extends downward from the National Security Committee of Cabinet (NSC), through to the Secretary's Committee on National Security (SCNS) and on to the various departments that are responsible for determining intelligence directions and collection priorities at lower levels. Involved departments include the Department of Defence (DIO, DSD and DIGO), the Department of Prime Minister and Cabinet (overseer of ONA), the Department of Foreign Affairs and Trade (DFAT, which currently "hosts" ASIS) and the Attorney-General's Department (AG, which currently has policy responsibility for ASIO).

The Flood Inquiry recommended the development and implementation of a community-wide collection management strategy and that the national and Defence priority systems be integrated (Flood, 2004, pp. 64-65). The loose collection of intelligence organisations and systems within the AIC has given an inordinate degree of latitude with intra-agency task prioritisation and collection assignment. It is vital that a national mission management system and control centre be constructed which can input, monitor, and account for the satisfactory tasking and completion verification for any given intelligence requirement within the AIC (Figure 3). The centre should be capable of handling routine, ongoing intelligence tasking as well as emergency, "ad-hoc" type tasks. A centralised centre and system will ensure that the collectors themselves are not forced into the difficult position of deciding between the needs of different clients (Flood, 2004, pp. 63-64). The informal means by which clients and collectors exchange information is of high value and can be maintained, while communicating priorities, tasking and feedback through an established collaborative system.

It is vital that a systems development be sanctioned for a cross-community national mission management system (MMS). The master system should be located within a National Mission Management Centre (NMMC), the central source of national requirements and tasking insight (depicted within ONA in Figure 1). The Trans-

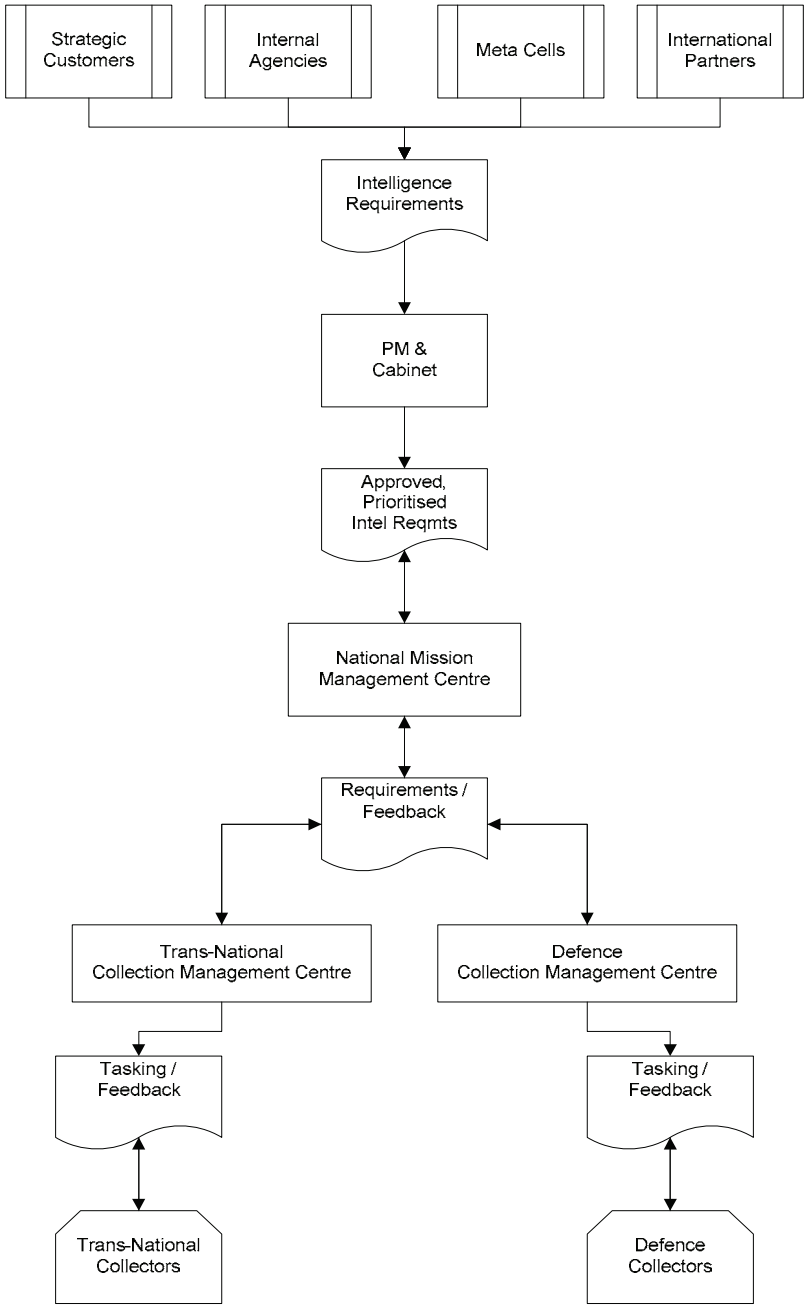

Figure 3 – Centralised AIC requirements, tasking, and feedback concept

National Intelligence organisations and Defence Intelligence organisations should each have their own Collection Management Centre and a MMS that replicates and communicates with the NMMC system and staff. Each key intelligence unit should also have a MMS terminal to receive tasking and to input their task status.

A standardised requirements and tasking nomenclature should also be developed for use across the entire AIC, along with a communications message series of templates that are agreed upon and used within the MMS. Sensitive tasking can also be accommodated in a variety of compatible ways. The system should be easy to use, intuitive, and reliable. The U.S., U.K., and certain programs within Australia have systems in use today which can be evaluated to gather ideas for an Australian mission management system design. A formal training program should be administered to all intelligence personnel requiring access to the MMS and access to the system should not be permitted until proficiency is demonstrated. Local branch chiefs should be held responsible for ensuring content and system usage continuity. There must be 100% personnel accountability and task traceability in the new AIC. Additionally, the Inspector-General of Intelligence and Security (IGIS) organisation should also have a MMS terminal for monitoring of requirements management, task collection traffic and calculating AIC performance metrics.

Intelligence tasks can become saturated with unwarranted collection, "lost in the system", or have already been collected and reported upon but the systems in use today do not afford the insight required for efficient requirements-collection-product provision operations. Current systems are a blend of tools varying from a

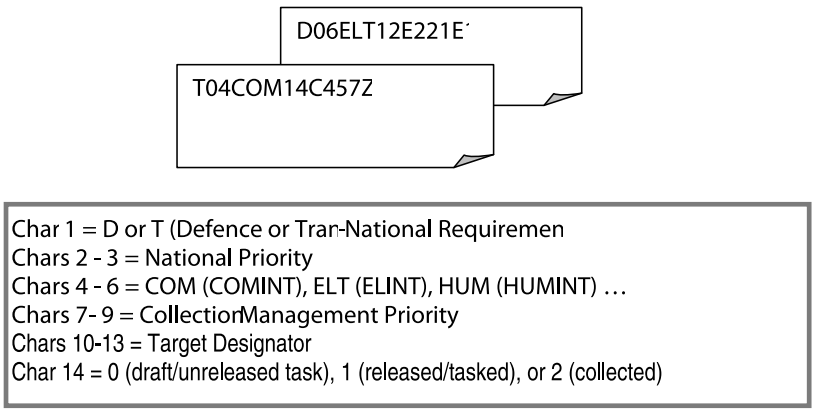

Figure 4 – Standardised intelligence requirements & tasking nomenclature (example)

customised priority management tool (intermittently used and accessible to a segment of the community), specific task management tools (developed within individual intelligence centres), and a variety of Microsoft Office suite uses (such as Outlook). Australia must create a structure and process to facilitate communications between the requirement owners through to the analysts. Knowledge mining and discovery will be powerfully enabled through the implementation of a common nomenclature

across the AIC (example: Figure 4). These features must be built into the system and easy to use so it becomes a natural part of how the people in the AIC operate.

NEW TRANS-NATIONAL AND DEFENCE INTELLIGENCE CHIEFS

The AIC is composed of a number of sizeable organisations, each operating under an assigned organisational head. However, in the current structure, there is a distinct absence of a single intelligence chief who is responsible for pulling together and making sure that "related intelligence" units are operating as an integral unit; particularly in the multi-source, multi-faceted challenge environment the AIC faces today and in the future. This AIC organisational leadership requirement becomes quite clear when observing the number of independent chiefs the AIC has today, each enacting their own set of policies and procedures unique to their specific organisation.

A logical approach would be the creation of a Trans-National Intelligence Chief and a Defence Intelligence Chief position that will be responsible for related intelligence organisations. The Defence Intelligence Chief position may be a re-definition of the existing Deputy Secretary, Intelligence and Security position. These individuals would be the spokesperson for and accountable to the NSC for all matters relating to their organisations. They would have insight and oversight of cross-agency operations, processes, and issues, ensuring that all subordinate organisations are operating in accordance with "the master plan". ASIO, ASIS, and AFP need to work closer together to best strategise and address the mutual trans-national issues they face today. This could be accomplished through defined Trans-National chief-led processes and forums geared to enable collaboration and synchronisation. DSD, DIGO, and the other Defence organisations will also benefit from single point leadership and inter-agency/system planning while still being able to focus on their specific mission areas.

The Trans-National Intelligence Chief would be responsible for the following organisations activities as related to their involvement within the AIC:

- ASIO
- ASIS
- AFP Intelligence (Representation Cell)
- Customs
- Coast Watch
- DOTARS

The Defence Intelligence Chief would be responsible for the following organisations activities as related to their involvement within the AIC:

- DSD
- DIGO
- DIO
- Defence Special Operations

- Defence-owned regional/theatre intelligence centres (e.g. JOIC)
- Defence-owned other intelligence collection assets

Since the post-9/11 creation of the Director of National Intelligence (DNI) position in the U.S., a measure of progress has been made to improve information sharing procedures and formats between national-state-local area fusion centres, fostering collection and analytical transformation, and modernising business practices within the U.S. intelligence community (McNamara, 2008; McConnell, 2007; Negroponte, 2006). The U.S. Government Accounting Office (GAO), reviewing the DNI's Information Sharing Environment (ISE) program in 2008, believed that the ISE still had a long way to go in communicating with stakeholders and folding the required changes into an actual ISE design. They were also concerned with the lack of ability to measure performance improvement brought about by the implemented changes (U.S. GAO, 2008). The DNI, principal advisor to the President, the National Security Council, and the Homeland Security Council for intelligence matters related to national security, has purview over the sixteen member intelligence community. A Deputy DNI position, created to assist the DNI across a number of responsible areas (Negroponte, 2005), is filled by an active duty commissioned officer in the armed forces (usually four-star equivalent) or a senior individual who has had training or experience in military intelligence activities and requirements. An Australian leadership model should consider a recommendation of separate directors for trans-national and defence intelligence. I believe that the magnitude and diversity of responsibility for their respective intelligence activities (trans-national and defence operations related) warrants the co-sharing of responsibility by knowledgeable intelligence professionals at the peak of expertise. The leadership candidates for these positions should be selected from the senior cadre within the intelligence field. They should possess the correct experience and skills set to judiciously and equitably administer the office and should not simultaneously occupy another intelligence community leadership position. These two leaders must work together to drive the AIC toward constructive transformation.

Each year, the Trans-National and Defence Chiefs should present a document to the NSC that would highlight what their organisation believes is required and what they are planning to do. The intelligence consumer is often unable to forecast what they require until they actually need it. This should open up a dialogue with the consumers and solicit their feedback before the community commits funds toward any particular direction (Kinsvater, 2003, pp. 3-5). This would also provide clear insight into trans-national and defence related budget priorities.

The purpose of creating the two new leadership positions is to facilitate the AIC becoming an integral, adaptive, purpose-designed organism, not the sum of individually operating parts. The intention is not to create another layer of bureaucracy but to effect transformational change. An orchestra requires the direction of a conductor who is in tune with all the various sections within the symphony. If there were conductors for each section of an orchestra, the likelihood of lost synchronisation, resultant noise, and confusion would be greatly increased. The AIC is akin to an orchestra; each organisation is assigned a specific set of responsibilities

which must blend seamlessly together with the rest of the community. This requires continuous, macro-level leadership which, apart from today's periodic committees and investigations, is missing within the existing AIC. A Trans-National Intelligence Director and a Defence Intelligence Director can be responsible for synthesizing interaction and driving cross-community vision.

DFAT

The current Department of Foreign Affairs and Trade's (DFAT) stated mission (http://www.dfat.gov.au/, 2007, para. 5) is "to advance the interests of Australia and Australians internationally. DFAT works with allies and partners to confront terrorism and to enhance counter-terrorism cooperation to provide greater security for Australians at home and abroad." The role of a foreign affairs and trade organisation would best be fulfilled by an organisation that does not have the country's foreign espionage organisation, ASIS, within its portfolio. The handshake of diplomacy, honesty, and trust does not attach well to the body of spying, misinformation and deception. De-coupling DFAT from ASIS ministerial oversight responsibilities would maintain an "honest broker" face to the international community and would keep Australian embassies from becoming or being perceived as covert or military "special operations headquarters", a contemporary problem for other countries. It would best serve the diplomatic and trade agency of Australia to only be involved with diplomatic and open source reporting, the volume of which currently outweighs conventional assessed intelligence by a factor of twelve (Flood, 2004, p 92). This change would also lighten the DFAT minister's workload which has significantly increased in recent years due to the rise in defence and counter-terrorism issues (Flood, 2004, p. 52). DFAT would continue to provide advice for people travelling overseas about specific security threats abroad and the role of Australia's embassies and consulates. DFAT would also continue to provide information in relation to the protection of foreign dignitaries. All-source intelligence assessment would be available to DFAT, as required, through NMMC tasking and ministerial membership within the NSC of Cabinet.

The ASIS responsibilities are typical of other HUMINT organisations: intelligence and counterintelligence operations, strategic deception, misinformation, as well as the associated science and technology development. The Australian Secret Intelligence Service (ASIS) should be placed under the Trans-National Intelligence organisation, encouraging better cooperation with ASIO, Defence, ONA and AFP on mutual tasks within the same structure and a common intelligence-professional chief. ASIS covert staff and activities can be protected as they are today, but their regulatory control and interface would be supervised under an intelligence-centred organisation, not the Australian diplomatic and trade corps.

DFAT embassies and consulates would most likely be briefed on regional operations and called on to provide administrative support to ASIS operations; however, DFAT would not be ministerially responsible for foreign intelligence agency operations. DFAT would continue to run the Australian Safeguards and Non-Proliferation Office

(ASNO), which regulates nuclear safeguards within Australia to ensure that Australia meets non-proliferation treaty commitments and implements the Chemical Weapons Convention and Comprehensive Test Ban Treaty. ASNO would also remain involved in the development of domestic verification arrangements for the Biological Weapons Convention.

ATTORNEY GENERAL

This restructure suggests the movement of the Australian Security Intelligence Organisation (ASIO) from the Attorney General's portfolio to the purview and responsibility of the Trans-National Intelligence Chief. This will greatly facilitate the sharing of intelligence between like-divisions under the same roof (ASIO, ASIS, and an AFP Intelligence element).

The Attorney General's Office should continue its primary role of providing the Australian government with legal advice. There must be a more detailed analysis prior to determining the logical placement and management of other important responsibilities such as Emergency Management and Response, the Protective Security Coordination Centre (PSCC), and the 24 hour Watch Office functions. On the surface, it may make sense to relocate some of these functions, along with the ASIO organisation, under the Trans-National Intelligence organisational umbrella. The PSCC chairs the Australian Government Counter-Terrorism Committee (AGCTC), a forum which shares relevant information among member agencies and reviews the level of national counter-terrorism alert. The AGCTC also develops whole of government advice in relation to counter-terrorism arrangements. The Committee includes representatives from Australian Government security, law enforcement, intelligence and emergency service departments and agencies (http: //www.ag.gov.au/www/agd/agd.nsf., 2007).

AFP INTELLIGENCE ELEMENT – PERMANENT INCLUSION

The addition of an Australian Federal Police (AFP) Intelligence element within the Trans-National Intelligence organisation would empower the sharing of timely information between co-players who are attempting to meet many of the same challenges. Intelligence-led policing (ILP), a model of policing which focuses on the use of criminal intelligence to systematically analyse and guide operations in the field, began to appear in Australia in the late 1990s (Ratcliffe, 2003, pp. 2 & 5). Rather than reactively responding to individual incidents, systematic analysis is conducted of offences that identified patterns and problem areas (NCIS, 2000, pp. 8-9). Police provide this information to patrol officers, detectives, management, and other participating personnel and agencies on specific criminals, crime groups, and criminal activities. Police intelligence centres search numerous public and private databases to gather and analyse information. They also generate intelligence products of their own, providing overviews of terrorist or other crime groups, analysis of trends, and other items of information for dissemination to participating agencies. AFP liaison officers are located around the world in twenty-seven countries as part of

the AFP's International Network. Australian police officers work with overseas law enforcement authorities to protect Australia's interests and provide a valuable range of services to all the AFP's activities (AFP, 2007, p. 4).

One of the major issues raised internationally by police officers (Peterson, 2005, p. 4) is the belief that, in order to be effective in preventing terrorism and related criminal activity, it is essential that they fully participate in the intelligence cycle at both the federal and non-federal levels and become advocates for law enforcement intelligence products that meet their requirements. The AFP should be able to submit collection requirements for prioritisation alongside of other national requirements, just like Coastwatch, Customs, or DOTARS. When intelligence product is generated which satisfies a non-AFP requirement but also satisfies an AFP requirement, the product should be able to be forwarded to the appropriately-cleared police consumer. Further integration of the AFP into the AIC would help develop and coordinate the necessary systems, processes, education, training, and professional services required for a unified Australian approach to providing the AFP with the best possible intelligence. Incorporating privacy and civil liberties protection under the advice of the Attorney General, the Australian Government should establish this permanent bridge between intelligence and law enforcement. Appropriate policy and processes can be established for transitioning from intelligence collection to evidence collection. The current NTAC does have an AFP representative, but this is a far cry from full integration. The world today places the "cop on the beat" on the front lines of intelligence collection and operational response. They are the eyes and ears of the neighbourhoods, commercial centres, and industrial estates. Information must flow rapidly in both directions to advise, protect, and support their operation. The AIC should take the logical step of amalgamating a representative group from AFP intelligence into the Trans-National Intelligence organisation.

Another information sharing challenge cited by law enforcement officers is the lack of sufficient amounts of specific and actionable information that might help them detect and prevent a potential attack (Committee on Homeland Security, 2006). The newly formed AFP intelligence element would be able to facilitate information sharing and ensure that law enforcement intelligence is written in a way that is actually useful to police and border patrol officers. The assignment of appropriately cleared state and local police officers to the Trans-National intelligence organisation would help intelligence analysts identify what threat-related intelligence is actually of interest to local law enforcement, help produce reports which can be disseminated to officers in the field, and serve as a point of contact for law enforcement agencies and officers who have information to share with the AIC.

There should be further analysis accomplished to define what element of the AFP should be represented within the Trans-National Intelligence organisation and the nominated individuals should be given the appropriate security clearances. Additionally, where intelligence information cannot be "sanitised" to an unclassified law enforcement sensitive level, law enforcement executives should be given security clearances so they can access data that is relevant to protecting people and places within their jurisdictions (Committee on Homeland Security, 2006). While state, territory and

local police forces would not necessarily have to be physically represented in the AIC AFP element, they would be able to interface with the proposed AIC AFP element as mission management and dissemination systems enhancements could accommodate formatted requirements, tasking, tip-offs, and analytical reporting. There may be additional knowledge sharing benefits for AIC secondments of state and local police representatives to further close the gap between the intelligence community and the police.

IGIS

The current role of the Inspector-General of Intelligence and Security (IGIS) is to provide independent assurance to the Australian Government, the Parliament and the people that the Australian intelligence and security agencies conduct their activities within the law, behave with propriety, comply with ministerial guidelines and directives and have regard to human rights (http://www.igis.gov.au/, 2007). The IGIS is a key element of the accountability regime for Australia's intelligence and security agencies:

- Australian Secret Intelligence Service (ASIS)
- Australian Security Intelligence Organisation (ASIO)
- Defence Imagery & Geospatial Organisation (DIGO)
- Defence Intelligence Organisation (DIO)
- Defence Signals Directorate (DSD)
- Office of National Assessments (ONA)

The Flood Inquiry (Flood, 2004, p. 61) recommended that the Foreign Intelligence Coordination Committee be established to assist the Director-General of ONA in coordinating, monitoring and reporting on the performance of the foreign intelligence community. While this positive recommendation has been implemented to a certain extent, further expansion of community-wide performance measurement and improvement is required. A committee is probably not an appropriate mechanism to accomplish the community assessment with the regularity required across such a large establishment as the AIC. To accomplish this, the IGIS role in the recommended future AIC structure would be expanded to include the measurement and evaluation of AIC enterprise performance. System insight would be provided through the provision of a Mission Management System (same real-time system MMS used by the NMMC, the Collection Management Centres, and collection/production locations) through which IGIS staff would be able to track the life of requirements through to consumer product provision. Over time, metrics could be established across the various task types and performance statistics would be revealed. Announced and unannounced operational test tasks/scenarios pre-coordinated with the Trans-National and Defence Intelligence Chiefs would be run and feedback provided to the Chiefs and organisational members for lessons learned and system/process improvement. The IGIS role would increase in community-wide importance as the "AIC system" would

continually be improving from real benchmarking, metric performance measurement and evaluation, and process improvement.

The instantaneous response by the AIC staff to an increased IGIS role, particularly the organisational heads, would probably be one of scepticism. An IGIS role expansion can be construed as unwarranted incursion into intelligence operations by unqualified staffers with nothing better to do (or an axe to grind). However, with the right approach, charter, and staffing, the IGIS would become a vital cross-agency link to assist in the identification of enterprise system problems, process bottlenecks, and requirements/tasking issues that may be undetected or not addressed.

While the current IGIS remit does not include efficiency, effectiveness or "second guessing" key judgments in assessments, this must change. The "second guessing" statement will always be an allegation of any evaluation an organisation undergoes. The IGIS, working closely with the involved organisations, can make sure that observations and measurements accurately reflect system and process performance. A "trusted agent" from each affected organisation could be included as part of each IGIS evaluation team to make sure that the data is being interpreted correctly and all influencing variables have been taken into consideration.

The AIC must employ a cross-community agency who will be responsible for keeping performance across the entire enterprise accountable. The IGIS office is well-positioned and should be given the appropriate authority and budget to accomplish this role. Suitable personnel would be required to fill the new measurement and evaluation positions.

DIRECTORATE OF INFORMATION ACCESS AND MANAGEMENT (DIAM)

There is a pressing need to create a directorate within the AIC to work together with the Defence Chief Information Officer Group (CIOG) and other related AIC entities to strategise and direct the AIC information access and management enterprise.

AIC producers and consumers must be able to access the intelligence they need when they need it. Sharing information is an issue much bigger than the Information and Communications Technology (ICT) field. Some organisations still run legacy systems that were planned and in some cases deployed prior to the internet. The systems were not built to talk to one another and the technical challenges involved with making them communicate are daunting. This demands vast resources to synchronise various systems and to keep them secure while modernising ICT facilities and infrastructures. There is also a lack of secure physical space to hold the equipment and the people to run it, especially in cramped headquarters buildings in Canberra where the AIC is struggling to seat new analysts, officers, and administrative personnel. Organisations are still reluctant to share intelligence information. In some cases this reluctance stems from concern about protecting sources and methods (Office of the Director of National Intelligence, 2007). Information-sharing and releasibility will involve policy changes, including sharing information with non-Commonwealth partners and the private sector.

The proposed AIC structure creates a directorate responsible for planning and guiding the execution of the ICT enterprise across the AIC. The Directorate of Information Access and Management (DIAM) would inventory the AIC architecture to strategise the development and provision of cross-domain solutions that enable the AIC systems to move information between networks operating at different security classifications, thereby improving collaboration and sharing.

The DIAM would be responsible for strategising, planning, and managing the following areas within the AIC:

- Movement, storage, and management of content
- Collaboration and data sharing
- ICT Standards
- Communications
- Network access, security, and management
- Configuration management
- Open source intelligence product repository.

As Australia continues to build international intelligence relationships, we face the issue of how to set policies to expand and govern sharing of information and secure network access with intelligence partners. The DIAM Chief must work to establish clear, uniform ICT security practices and rules that allow us to work together for the protection of Australia's secrets.

There must also be a concerted effort to address community-wide handling of open source intelligence. Each organisation within the AIC has been challenged, to a certain extent, with the growth within the open source domain. The DIAM, along with the Trans-National and Defence Intelligence analytical representatives, should conduct a cross-AIC forum to discuss alternative AIC approaches to this burgeoning area. The U.S. is implementing a document and media exploitation (DOMEX) centre under the new Director of National Intelligence (DNI) organisation (U.S. Intelligence Community, 2007). The DNI has also created a new position, Assistant Deputy Director of National Intelligence for Open Source (ADDNI/OS) to oversee the open source activities. Australia might consider the feasibility of a centralised entity in the new AIC future structure. This could be the positive step towards a centralised policy, process and repository to guide AIC entities in the search, validation, format, deposit, and management of open source intelligence (OSINT).

There are a number of ongoing AIC efforts to fuse information databases from all-sources into data warehouses and run search engines and other knowledge management tools over the top of the data. This is a departure from the individual agency, member-based system approach. The movement is progress toward a fusion centre approach to data alignment and sharing. The questions of data access and privacy when potentially merging individual-specific or cross-organisation information are issues that must be addressed by the AIC. There should be methods developed to control data access when fusing data. The AIC should be able to identify components of the fused data that belong to the originating agency. In a data warehouse containing

data from intelligence agencies, AFP, Customs and Defence agencies, tools could be devised that would allow each agency to view the other organisation's data according to the governing rules that apply.

The DIAM would also be responsible for evaluating the AIC communication networks' usage and integrity. The AIC is currently serviced by a variety of networks, but AICNET is the most important (Gordon, 2005, p. 52). AICNET is a secure communications network which functions as a communications system and data warehouse. AICNET has in-built capabilities to sort information around specific topics with the ability to retain communications, intelligence reports and information. Other communications and data systems also exist outside the AIC such as the AFP case management system, called the Police Real-time Online Management Information System (PROMIS). PROMIS is both a communications system with secure email and a database for maintaining intelligence and investigations records. The ability of the AIC to access intelligence information within multiple systems across firewalls, interfaces and security zones will continue to be a key challenge area for a DIAM Chief and the Community at large.

TAG AND DIO ANALYTICAL ORGANISATIONS

Within the new AIC structure, traditional analytical responsibilities will continue but would be supportive of the new meta cell framework. Long term strategic assessment and ongoing analytical activities would continue to be accomplished by analysts remaining within ONA, TAG and DIO. Their activities would be either unique to or in support of meta cell activities. The latest assessment of a country across political, economic, military news and situation reporting would be continually available to AIC headquarters and in-theatre authorised consumers via a central Knowledge Discovery Database (KDD) building on the existing "intelpedia" concept. For all KDD entries, users could receive an update notification to alert authorised users of a new product posted from that country, region, or target set. The volume of data continues to grow and the AIC is going to have to rely on better tools and processes to enable product archiving, key word searches, etc. Technological requirements would be defined through collaboration with the DIAM directorate.

PERSONNEL AND TRAINING

The recruiting shortages within the Australian Defence Force, coupled with the retirement exodus of a growing number of experienced intelligence public service professionals, will further emphasize the need for people and better tools. New strategies, such as augmentation with private enterprise personnel, should be investigated to assist the AIC with the growing amount of time-consuming analytical work. Collection management, remote sensing, linguistic support, document exploitation, training and technical analysis are some AIC support functions which could be performed by private contractors. Australia must clearly define the role and structure of intelligence community outsourcing. A U.S. Army paper (Voelz, 2006,

p. 2) evaluating the use of commercial augmentation for intelligence operations points out that:

> "As critical intelligence requirements are increasingly resourced through commercial augmentation, leadership must determine the appropriate roles for private sector firms and provide effective plans for legal oversight, operational integration, and management of contracted support".

The AIC must promote experienced analytical leadership who can match and balance skill-teams, not leaving groups of inexperienced, new analysts by themselves to figure things out or "wing it". This could include senior staff being rotationally assigned for short periods to 24/7 watch centres to share their experience and informally mentor less experienced personnel.

A standardised analytical front-end training course (e.g. Analysis 101) and through-career development courses should be offered to teach critical thinking, intelligence-cycle skills, knowledge and supervisory management. An AIC Training Directorate should be created to develop and administer cross-community training modules for personnel. Additionally, the institutionalisation of a formal "intelligence analysis" career path will help to keep experienced analysts directly involved with doing what they want to do – analysis. Traditional intelligence skilled people are battling for long-term relevance as the community is experiencing, in the words of Allan Behm, the "de-professionalisation of intelligence" phenomenon (Behm, 2007, p. 7). Analysts should be able to continue to have promotional opportunities within their specialised field, without having to career broaden out of the intelligence analysis field to achieve promotion.

KNOWLEDGE MANAGEMENT ENTERPRISE

The following diagram (Figure 5) depicts a conceptual Knowledge Management Enterprise that could be considered as a mechanism to facilitate and control the exchange of information (Zhou et al., 2004). The DIAM, TAG, DIO and NMMC personnel would be responsible for coordinating the design and implementation of a new enterprise architecture and AIC Information Centre, as well as the active management of an intelligence product repository and the systems to facilitate workflow and process.

The change presented in this conceptual future vision would modify the way the AIC currently functions, would put two senior individuals in charge of logically-affiliated organisations, and would centralise major Australian security issues into consolidated national intelligence cells based on mission or situation (centralisation) instead of the type of collection or agency. The national situation cells would be staffed by a cross-section of personnel seconded from the various AIC organisations (decentralisation), based upon their specific expertise. Each cell would represent a living "complex adaptive entity" able to be tailored to the specific mission challenge and disbanded when no longer required. Career incentives should be offered to individuals completing national cell duty.

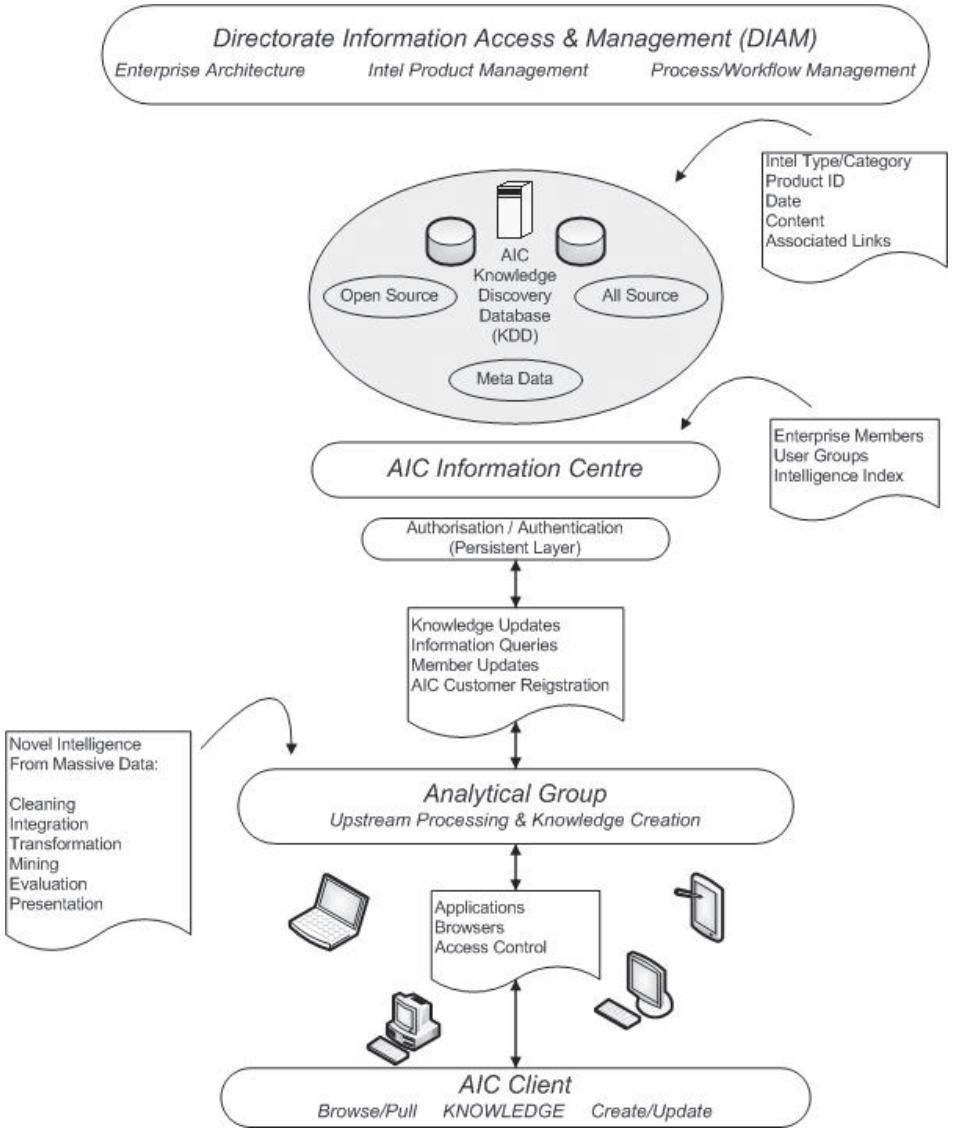

Figure 5 – Conceptual knowledge management enterprise

The new enterprise would create a central repository for intelligence information and create processes for active management of the tasking and product data flow. It also recommends expanding the role of ONA into a leading organisation integrally involved with and comprised of entities from across the AIC. It would also put in place, for the first time, an organisation with an ongoing charter to measure AIC performance.

THE WAY AHEAD

An action plan is a key management strategy that could be used to define a new AIC vision with strategic objectives, and purposely design the best way to secure and

present reliable intelligence in the 21st century. The future planning of the AIC is too important to be designed via the current fractured approach to upgrade projects which are independently planned by each AIC organisation. Too often has the AIC, due to time-job load constraints or lack of enduring motivation, merely identified the general requirements of a subsystem upgrade and handed the project over to acquisition and engineering technologists to come up with solutions. While technologists are beneficial at the appropriate stage of system development, they should not be left to design the AIC autonomously. Without a concentration of intelligence field literacy and experience, the technology, not the practitioner, will become the driving force.

An independent AIC team comprised of intelligence specialists (present and past) should be tasked to re-look at the design of the AIC, make recommendations and organise the requirements into an actionable plan. The team should collaborate with the various AIC organisational elements as necessary, but the design should not be left in the hands of any single AIC organisation. It must take a working view of the collaboration, processes, and structure required of the AIC and come up with alternative improvements to each of those elements. This larger vision must be initiated, mandated and driven from the highest level to ensure the process does not get commandeered along the way through tradition, culture or predisposition.

Unfortunately, a myopic community approach will cause the AIC to fall short of providing the Australian leadership and public with the best intelligence assessment, and ultimately the best national security protection for the dollars being spent now and in the future. Unchanged, the budget will continue to be spent on sustaining the multitude of disparate systems that service an awkward, stove-piped structure.

It is time for Australia to make an imprint on the future of Australian national security by modernising legacy structures and processes through the implementation of collaborative connectivity, knowledge mobilisation, multi-skill mixing and adaptation. Cross-community mission management tools must be developed to empower inter-operability and performance management. An agile and responsible intelligence community is essential if Australia is to overcome increasingly complex challenges in the future. Australia appreciates the benefits of multilateral security and intelligence sharing arrangements, but this is not a substitute for realising the opportunity to transform the AIC into a world-class, innovative intelligence apparatus.

References

Australian Federal Police. (2007). *AFP annual report: 2006-07 executive review*. 4.

Australian Government. (2007). *About inspector general of intelligence and security IGIS*. Retrieved November 12, 2007, from http://www.igis.gov.au/about.cfm.

Australian Government. (2007). *Australian government attorney general's department* (AGD). Retrieved February 20, 2008, from http://www.ag.gov.au/www/agd/agd.nsf.

Australian Government. (2004). *Report of the inquiry into the Australian intelligence agencies (Flood Report)*. Canberra: Department of Prime Minister and Cabinet.

Australian Government. (2007). *What we do – Our role and assets: Department of Foreign Affairs and Trade*. Retrieved January 23, 2007, from http://www.dfat.gov.au/dept/whatwedo.html.

Behm, A. (2007). *The Australian intelligence community in 2020*. Security challenges (Kokoda Foundation) 3, No. 4(7).

Chesterman, S. (2006). *Shared secrets: Intelligence and collective security*. Lowy Institute for International Policy Paper, No. 10(1).

Committee on Homeland Security. (2006). *LEAP: A law enforcement assistance and partnership strategy: Improving information sharing between the intelligence community and state, local, and tribal law enforcement*. Retrieved January 27, 2007, from http://www.hsc-democrats.house.gov/SiteDocuments/20060927193035-23713.pdf

Cotton, J. (2006). *Australian foreign policy and the management of intelligence post-September 11*. Asia Pacific School of Economics and Government, Australian National University Paper, PDP06-03.

Dilnutt, R. P. (1999). *Knowledge management as practiced in Australian organisations: A case study approach*. Southern Cross University. PhD Thesis.

Domestic Social Policy Division. (2007). *Intelligence and information-sharing elements of S. 4 and H.R. 1 (Rl34061)*. Washington D.C.: Congressional Research Service.

Dudgeon, I. (2006). *Intelligence support to the development and implementation of foreign policies and strategies.* Security Challenges (Kokoda Foundation), Vol 2(2).

Fourman, M. (2002). *Informatics*. Informatics Research Report EDI-INF-RR-0139. Edinburgh: Division of Informatics, University of Edinburgh.

Gordon, S. (2005). *Re-shaping Australian intelligence*. Security challenges (Kokoda Foundation). Vol.1(10).

Hakannsson, H., & Snehota, I. (1995). *Developing relationships in business networks*. London: Routledge.

Hellgren, A., Leif, M., & Leif, B. (1993). Structure and change: The industrial field approach. *Advances in international marketing journal* 5. (No. D), 87-106.

Iowa Public Safety Department. (2005). *Iowa fusion center concept dept of public safety*. Retrieved February 23, 2008, from www.iowahomelandsecurity.org.

James, N. (2004). *How to reform our intelligence agencies*. Retrieved February 6, 2008, from http://www.theage.com.au/articles/2004/05/06/1083635277388.html?from=storyrhs

Kinsvater, L. (2003). The need to reorganise the intelligence community (unclassified edition). *Journal of the American Intelligence Professional – Studies In Intelligence*, 47(1), 3-5.

Krono, N. (2007). Australia's response to terrorism – Strengthening the global intelligence network. *Centre for the Study of Intelligence* (CIA), 48(1).

Lievesey-Howarth, R. (1997). Electronic governance: The risk to society. *The Australian*, pp. 32-33.

McNamara, T. (2008). *2008 Annual report to the Congress on the information sharing environment (ISE).* Washington D.C.

Milner, E. (2000). *Managing information and knowledge in the public sector*. London: Routledge.

National Criminal Intelligence Service (NCIS). (2000). *The national intelligence model.* London: NCIS-UK.

Negroponte, J. (2006). *An overview of the United States intelligence community*. Retrieved July 23, 2008, from http://www.dni.gov/who_what/061222_DNIHandbook_Final.pdf.

Negroponte, J. (2005). *Office of the director of national intelligence, intelligence community policy memorandum number 2005-100-1*. Retrieved July 23, 2008, from http://www.fas.org/irp/dni/icpm/2005-100-1.pdf.

Oatley, C. (2000). *Australia's national security framework – A look to the future*. Australian Defence Studies Centre, Working Paper 61.

Office of the Director of National Intelligence. (2007). *500 day plan: Integration and collaboration*. Washington D.C.: Director of National Intelligence.

Peppler, B. (2006). *The future of intelligence*. Intelligence 2006 conference – Summary paper. Australian Homeland Security Research Centre Security Practice Note (November Issue).

Perez, P., & Batten, D. (2006). *Complexity science for a complex world: Exploring human ecosystems with agents*. Canberra: Australian National University Press.

Peterson, M. (2005). *Intelligence-led policing: The new intelligence architecture*. U.S. Bureau of Justice Assistance Paper. NCJ210681.

Poulton, E. (1994). *Behavioral decision theory: A new approach.* New York: Cambridge University Press.

Ratcliffe, J. (2003). *Intelligence-led policing*. Australian Institute of Criminology No. 248.

Rudd, K. (2008). *Joint statement with Prime Minister Yasuo Fukuda of Japan and Prime Minister Kevin Rudd, on comprehensive strategic, security and economic partnership*. Retrieved July 14, 2008, from http://www.pm.gov.au/media/Release/2008/media_release_0309.cfm

U.S. Government Accounting Office. (2008). *GAO report to congressional requestors – Information sharing environment (ISE) (GAO-08-492).* Washington D.C.

U.S. Intelligence Community. (2007). *Document and media exploitation – DOMEX (intelligence community directive number 302)*. Washington D.C.: U.S. Intelligence Community.

Voelz, G. J. (2006). *Managing the private spies: The use of commercial augmentation for intelligence operations.* Center for Strategic Intelligence Research, U.S. Joint Military Intelligence College Discussion Paper No. 14(2).

Waldrop, M. M. (1992). *Complexity: The emerging science at the edge of order and chaos*. New York: Simon and Schuster.

Welch, C., & Wilkinson, I. (2000). *From AAR to AARI? Incorporating idea logics into network theory*. University of West Sydney: Nepean.

Wilkie, A. (2004). *Axis of deceit: The story of the intelligence officer who risked all to tell the truth about WMD and Iraq*. Melbourne: Black Inc.

Zhou, M., & Hall, W. (2004). *Managing complex engineering knowledge in a distributed enterprise.* SESA (Systems Eng Society Australia – Victoria Chapter) Presentation. SESAVIC 27/07/2004.