Kokoda PAPERS

Getting it Right: Integrating the Intelligence, Surveillance and Reconnaissance Enterprise

NUMBER 18 April 2014

Gary Waters

Kokoda Paper No. 18
April 2014

GETTING IT RIGHT: INTEGRATING THE INTELLIGENCE, SURVEILLANCE AND RECONNAISSANCE ENTERPRISE

Gary Waters

The Kokoda Foundation

www.kokodafoundation.org

Researching Australia's Future Security Challenges

About the Kokoda Foundation

The Kokoda Foundation is a registered charity and not-for-profit organisation. Its research is independent and non-partisan. The Kokoda Foundation does not take institutional positions on policy issues nor do sponsors have editorial influence. Accordingly, all views, positions, and conclusions expressed in this publication should be understood to be solely those of the author.

Published in Australia by the Kokoda Foundation, April 2014.

National Library of Australia Cataloguing-in-Publication entry

Author:	Waters, Gary, 1951- author.
Title:	Getting it right : integrating the intelligence, surveillance and reconnaissance enterprise / Gary Waters.
ISBN:	9780980730678 (paperback)
Series:	Kokoda papers ; no. 18.
Subjects:	Military intelligence--Australia. Military surveillance--Australia. Military reconnaissance.
Dewey Number:	355.343

Series Editor: Catherine Scott
Publication Management: QOTE Canberra (02) 6162 1258
Printed by: Union Offset
Published and distributed by:
The Kokoda Foundation
2/10 Kennedy Street
(PO Box 4060), Kingston ACT 2604
T: +61 2 6295 1555
F: +61 2 6169 3019
Email: info@kokodafoundation.org
Web: www.kokodafoundation.org

Additional copies are available from the Foundation at
A$22.00 per copy (including GST and postage in Australia).

EXECUTIVE SUMMARY

Intelligence, Surveillance, and Reconnaissance (ISR) functions are essential for effective operations (encompassing military, border protection and law enforcement) and strategic decision-making. These functions provide greater situational awareness and better predictive intelligence necessary for superior decision-making at all levels. ISR synchronises and integrates the planning and operation of platforms, sensors, data and people.

Effectiveness of ISR depends on well-integrated technology and highly-capable people who constantly find new and innovative uses for that technology. Recruiting, training and retaining these people will be vital for dealing with the increasingly complicated challenges of the future.

The purpose of this Kokoda ISR Project is to develop new ideas for a future Australian ISR Enterprise that complements the emerging national security framework and positions ISR as a sovereign capability. Concerns have been expressed that the opportunities, challenges and risks confronting the national ISR community have increased and become more diverse in recent years. Consequently, the potential for extending the current Whole-of-Government approach to exploiting ISR and better accommodating Industry into the national ISR infrastructure needs to be explored. Innovation and integration of new ISR methods, systems, and concepts will be important for future success.

For the immediate future, Australia's military and law-enforcement organisations will need to embrace strategic, operational, organisational, technological, process, and cultural change in a tough fiscal climate, and demonstrate how they can achieve more with existing capabilities and organisations. They will need to meet the public expectation of effectiveness, responsiveness and accountability, and a well-integrated and robust ISR function will be critical in this respect.

ISR must be treated as an integrated process, moving it in complexity, speed, and effectiveness beyond the current model of

inter-agency cooperation. Indeed, cooperation, coordination and interoperability are no longer enough: collaboration must be the order of the day.

The ISR Enterprise is now undertaking a much broader range of functions across increased areas than in the past. Indeed, the ISR function and its community represent a national capability, which means all efforts should come together in a whole-of-nation approach that brings in industry, academia, State jurisdictions and Federal agencies. This demands a strategic design from the outset and a new culture around closer collaboration.

It is vital for public engagement to be improved - the social balance between expectations of actions for security and the need for privacy must be struck if the ISR Enterprise expects to retain any form of social licence. Greater transparency of the checks and balances imposed on the ISR Enterprise can lead to a substantial increase in the level of trust from the public.

It is also vital to deal with the increasing volume of data, as well as its variety, velocity and variable veracity to extract greater insights and more reliable prediction of events. Accelerating the data-to-decision cycle would allow faster transition from collection to analysis, decision and action; and greater confidence in the analysis, decisions and actions.

It is crucial to synchronise the development of ISR capabilities, which demands from the start, a multi-disciplinary approach to collection. Greater synchronisation of ISR capabilities would support the other policy objectives of adopting a whole-of-nation approach, improving public engagement, and accelerating the decision-to-action cycle.

From a strategic design perspective, Australia should align its vision, governance, infrastructure, data, and workforce across the ISR Enterprise. This is needed to meld with the emerging national security framework as it copes with the whole-of-government (and whole-of-nation) approach to handling crises. This alignment is also needed to meet the continuing tight national fiscal situation that will demand

an evaluation of priorities for all ISR agencies, including how they collaborate and how they invest in and synchronise their capabilities.

All of this will place different demands on the workforce and the ISR Enterprise needs to be investing now in new competencies; improving workforce skills; and better coordinating the workflow of people, resources and materials.

This *Kokoda Paper* acknowledges the need to pursue the current trajectory in making the most of Australia's organisations, capabilities, and international and national cooperation. But it also recommends four policy approaches that should be pursued - adopting a whole-of-nation approach, improving public engagement, accelerating the data-to-decision cycle, and synchronising ISR capabilities – and outlines specific proposals within each of these areas.

ACKNOWLEDGEMENTS

This publication would not have been possible without the support and assistance of several departments and agencies within the national security community and ISR community more specifically, as well as a range of industry representatives. The senior officials and industry leaders who participated in the ISR project provided exceptional insight and assistance. A significant number of interviews and meetings and several workshops were conducted throughout 2013 and the Kokoda Foundation would like to thank all of those involved in these various activities.

The Project would not have been possible without the generous support of our sponsors – BAE Systems and Northrop Grumman – who also provided sterling assistance in offering detailed briefings and discussions on key aspects of ISR.

BAE SYSTEMS

NORTHROP GRUMMAN

The Kokoda Foundation is also grateful to the initial team led by Ian Gordon and John Oddie for conducting the first tranche of interviews and running the first workshop. Alex Tewes also provided outstanding assistance in helping to set the scene from this earlier work and for contributing to defining the direction of the remaining work.

As this report was being finalised in the first two months of 2014, Ross Babbage, Bill Osborne and Steve Zanias provided wonderful assistance in helping to focus and smooth the final product. I cannot begin to thank them enough for so willingly and graciously offering their valuable time so promptly when needed.

ABOUT THE AUTHOR

GARY WATERS

Dr Gary Waters spent thirty-three years in the Royal Australian Air Force, retiring as an Air Commodore in 2002. He subsequently spent almost four years as a senior public servant in Defence and then worked with Jacobs Australia as Head of Strategy for just over seven years. He left Jacobs in March 2013 and now acts as an independent consultant.

He has written thirteen books on doctrine, strategy, cyber security, and military history. His latest two books are 'Australia and Cyber Warfare' (with Professor Des Ball and Ian Dudgeon, 2008), and 'Optimising Australia's Response to the Cyber Challenge' (with Air Vice-Marshal John Blackburn, 2011). In early 2014, he also published his Kokoda Foundation Discussion Paper entitled 'Pressing Issues for the 2015 Defence White Paper'.

He is a Fellow of the Royal Melbourne Institute of Technology (graduating with majors in accounting and economics); a CPA; a graduate of the United Kingdom's Royal Air Force Staff College; a graduate of the University of New South Wales, with an MA (Hons) in history; a graduate of the Australian Institute of Company Directors; and a graduate of the Australian National University with a PhD in political science and international relations.

He has been a Fellow of the Australian Institute of Company Directors, a Vice President of the United Services Institute, and a Board member of Defence's Rapid Prototype, Development and Evaluation (RPDE) Program. He currently serves on the Board of the Kokoda Foundation.

CONTENTS

INTRODUCTION

Understanding the environment in which a conflict is being or will be conducted has always been a central element of military thinking. In today's world, this understanding is embraced by three elements: Intelligence, Surveillance and Reconnaissance (ISR). Whilst ISR has traditionally focussed on military operations, the last century has seen an increasing emergence of ISR as a construct and capability that might support a broader 'national interest'. Indeed, today the national security community is engaged as both a user and contributor, and the need has recently emerged for an ISR capability that supports border protection in which a 'national' or 'sovereign' interest, as opposed to a 'military' paradigm, has come to the fore.

Conceptually, an ISR capability allows for the observation and analysis of events and the production of useful, timely information to support a national interest. In reality, this simple ISR construct is challenged by several factors: the number of events; the ability to observe; processing the observed events and the increasing amount of data; the time taken to conduct an analysis; the time to determine a course of action; and the time taken to respond.

The simple ISR construct is further challenged when the many networked and linked sensors used to observe events are taken into consideration. Increased sensor inputs provide greater situational awareness and better predictive intelligence necessary to achieve superior decision-making and, hence, more effective operations. However, modern-day ISR systems have also significantly reduced the available time in the decision cycle for making sense of what is occurring and for carrying out an action as a result. The challenge, therefore, is to balance the greater situational awareness and better predictive intelligence with ensuring that decisions are not delayed waiting for additional information.

The purpose of this Kokoda ISR Project is to develop new ideas for a future ***Australian ISR Enterprise***[1] that complements the emerging

1 The ISR Enterprise comprises platforms, sensors, data and people.

national security framework and positions ISR as a sovereign capability. Concerns have been expressed that the opportunities, challenges and risks confronting the National ISR Community have increased and become more diverse in recent years. ***Consequently, the potential for extending the current Whole-of-Government approach to exploiting ISR and better accommodating Industry into the National ISR infrastructure needs to be explored***. Innovation and integration of new ISR methods, systems, and concepts will be important for future success.

For the immediate future, Australia's military and law-enforcement organisations will need to embrace strategic, operational, organisational, technological, process, and cultural change in a tough fiscal climate, and demonstrate how they can achieve more with existing assets and organisations. They will face challenges as they seek to cooperate more closely, yet feel the need to retain some of their traditional boundaries (noting that many of the traditional boundaries are set in legislation). They will need to meet the public expectation of effectiveness, responsiveness and accountability, and a well-integrated and robust ISR function will be critical in this respect.

This *Kokoda Paper* examines the nature of the ISR challenge confronting Australia and how that challenge is currently being met. It argues that an extension of current policy approaches that involve making the most of Australia's organisations, capabilities, and international and national cooperation is called for. It identifies those other key areas for improved policy and argues the importance of adopting a whole-of-nation approach, improving public engagement, accelerating the data-to-decision cycle, and synchronising ISR capabilities; and recommends specific proposals for pursuing these policy outcomes.

BACKGROUND AND CONTEXT

ISR is defined here as an activity that synchronises and integrates the planning and operation of platforms, sensors, data and people in direct support of the national interest which, in the context of this study, involves military, border protection and law enforcement operations.

ISR is an integrated function in which intelligence, surveillance, and reconnaissance are often referred to as a collective whole, though the capabilities are distinctive and each fulfils a different purpose.

The information derived from surveillance and reconnaissance, converted into intelligence by exploitation and analysis, is used to formulate strategy, policy, and/or operational plans; to develop and conduct campaigns; and to protect, prevent, and prevail against threats inimical to the nation and its interests.

While well-integrated ISR technology provides a clear advantage, so too does the ingenuity of the people who constantly find new and innovative uses for current and developing technology to provide a competitive advantage and enable them to achieve effects across military and law-enforcement operations (including customs, border protection and police operations). Recruiting, training and retaining highly-capable people who are attuned to dealing with modern-day challenges that grow more complicated year after year is a critical issue for future ISR success.

Individually and collectively, Australia's military, police, customs and like organisations have probably never faced the complexity of the challenges they face today. High levels of connectivity and improved efficiency through the availability of new and cutting-edge technology provide an ability to connect and collect information from both legacy and emergent systems in the military, public and private domains. Public expectations that citizens will be protected and that those who protect them will do so with high degrees of transparency and accountability simply add to this complexity. While the Australian Defence Force (ADF) has yet to address ISR as a unique military capability, Australia as a nation, likewise, ***has not considered ISR as a sovereign capability***.

At the tactical and operational levels there are substantial questions about access, control and ownership of platforms and systems; the standards under which they operate; and the sharing of data between first and subsequent users. At the strategic level the big questions involve organisational and system integration, the legislative framework, the international cooperative arrangements, and the funding and management paradigm for ISR.

These questions require answers and need to be addressed in a more integrated and synchronised way than currently. Taking such an 'enterprise' approach is necessary for the future ISR Community to be able to rise to meet the complex challenges of tomorrow and would ensure:

- greater engagement with the public (the public can also act as a resource);
- optimised ways of working in terms of effectiveness, efficiency and economy (which also involves looking at the workforce differently such as greater use of part-time and semi-retired people);
- empowered people (with real-time access to usable and actionable data);
- greater use of analytics to improve predictive capability and operations/services (providing greater awareness and more cost-effective use of resources);
- enhanced collaboration with like agencies (which will be difficult in a climate of competition for resources); and
- a proactive posture (anticipating developments and getting ahead of the changes so as to be less reactive).

THE NATURE OF THE ISR CHALLENGE

The goal of ISR activities is to provide accurate, relevant, and timely intelligence to decision-makers and operational commanders. This allows strategic decision-makers to determine the necessity of certain operations, and for operational commanders, it provides the intelligence and situational awareness necessary to successfully plan and conduct those operations.

This goal is becoming more complicated as national security becomes more encompassing, which imposes new and more diverse requirements on the ISR Enterprise. A tighter fiscal climate adds to this complication.

Policy and legislative barriers continue to pose an organisational challenge. Existing assets tend to be acquired for single agency

solutions. Cooperation has improved but still seems to be more of an add-on than an inherent part of a systemic culture. While these issues have been recognised and some modest progress has been achieved, more needs to be done in each of these areas.

The more problematic areas of concern are the lack of national collaboration across the ISR Enterprise, the weakening of social licence[2], the apparent inability to leverage commercial developments in speeding up the data-to-decision cycle, and the lack of synchronisation in developing future ISR capabilities. Pursuing the current trajectory will not resolve these concerns.

IMPROVING THE CURRENT TRAJECTORY

The current trajectory is achieving modest improvements in ISR, but more could be done in terms of: making the most of Australia's organisations (both public and private); making the most of existing capability; making the most of international relationships; and finally, making the most of national cooperation. These are addressed below.

Making the Most of Australia's Organisations

A key organisational challenge for Australia is to address the policy and legislative barriers that continue to conspire against achieving a seamless approach to national security and that compel agencies to operate within their own narrowly-defined contexts. Thus, different government departments and agencies continue to do essentially what they have always done, and no single organisation is building institutional capacity to ensure cooperation and collaboration in ISR to the extent that is necessary in the complex environment of the twenty-first century. Australia has a relatively small population in a vast continent, and as such, needs to leverage the best technology,

2 A distinction is made in this Paper between an externally-focused social licence (for surveying the Australian border outwards) and an internally-focused border-inwards approach. This is about a capability that helps Australia protect itself, not about a system for surveying citizens.

the best people, the best processes, and the best institutional arrangements to meet the goal of ISR activities described earlier.

One obvious way forward is to avoid duplication – it makes little sense, for example, to have a plethora of operations rooms around the country essentially performing the same task. The tight fiscal environment and continuing budgetary constraints will force the ISR Enterprise to make economies over time, and it would seem sensible for the various agencies to make the best choices possible before inchoate changes are forced upon them.

Making the Most of Existing Capability

Better utilisation of existing capability across the ISR Enterprise represents a real opportunity for protecting Australian sovereign interests. ***This would involve mapping the current ISR landscape to establish a solid foundation for the future positioning of ISR as a national capability***. Better integration of ISR capabilities will allow information to be shared and applied more diversely across the Enterprise, ensuring that decision-makers at all levels have access to the best possible information so that they can make the best decisions possible.

It is vital that the national effort leverages all contributions across the national security and intelligence milieu; as well as those that support national security in academic and commercial enterprises. This includes emergent technologies such as unmanned systems. There is already a proliferation of small unmanned system activities that should be coming together in a military context, a whole-of-government context, and a whole-of-nation context for an improved national ISR capability, particularly one that will need, increasingly, to support border protection activities.

Unmanned systems, particularly Unmanned Aerial Vehicles (UAVs) or Remotely Piloted Vehicles (RPVs), are being taken up for both commercial and other civil purposes within a mature and receptive regulatory context. However, the public perception in Australia, as in other Western nations, of unmanned systems is largely focused on UAV attacks on civilians in Afghanistan and Pakistan, as well as on the potential for unmanned systems to invade the public's privacy back

home. It is clear that significant public engagement will be needed to improve society's understanding of the use of unmanned systems in military and national security contexts.

While the wide adoption of unmanned systems might expand surveillance capacity significantly, the resulting information will not automatically translate into operationally-improved situational awareness. Analysis and dissemination of information requires specialised capacity depending on how the unmanned systems are to be used. Strategies will need to be developed around the transmission, storage and analysis of data from tactical, operational, strategic, and non-military unmanned systems. Increasingly, Australia should expect the focus of ISR to move from predominantly military operations to counter-terrorism and border protection operations. ISR will also evolve from being a support function to becoming an intrinsic element of all operations.

Making the Most of International Relationships

Cooperation in the capture, production, analysis and distribution of ISR products can be viewed as a commodity that when traded appropriately enhances Australia's relationship within the 'Five Eyes' community, and with traditional allies and regional partners. This has particular relevance in terms of sovereign border challenges.

Australia's engagement in the Middle East, working alongside the US military, and benefiting greatly from US-owned ISR assets, has resulted in the Australian military learning much about the operational benefit derived from access to a well-structured ISR capability. The increased presence of US military assets in Australia and the region will drive the need for ISR collaboration, specifically at an operational and tactical level with the US Pacific Command (PACOM).

Australia's location and presence in the Pacific provides an ideal land mass from which ISR sensors can be based, thus ensuring that Australia has something to offer in a partnership with other nations with interests in the Pacific. Exchange of information requires common frameworks and common interests. At program levels, Australian adoption of American and British technology means that standards are inherent in the acquisition. ISR by its nature operates

on multiple standards and domain frameworks that do not easily facilitate interoperability.

The rise and maturation of ISR as a capability in the United States has led to a drive towards an ISR standards framework that provides a mechanism through which ISR capabilities in the national security and military domains can interoperate. Similar ISR standards frameworks exist or are being developed in the United Kingdom, the North Atlantic Treaty Organisation (NATO) and the European Union. Notwithstanding Australia's partnership with the United States, a standards framework has yet to be developed, and more importantly the programmatic approach to ISR capability development seems to indicate multiple standards, with a consolidation path to be pursued at a later date. In essence, there is a real prospect of Australia retracing the American journey, at considerable cost in time and capability. Thus, ***Australia needs to select a standards framework to facilitate improved integration and collaboration***.

On the matter of collaboration, Defence partnership with the United States demands a highly sophisticated exchange, in which Australia's ISR contribution is likely to have significant benefit to the nation. Regional ISR collaboration is more likely to focus on border protection and law enforcement initiatives. Whilst the two relationships present different challenges, both have enormous advantages, particularly in the preservation of borders and in forming closer international relationships.

Making the Most of National Cooperation

The change in national security perspectives that arose following the terrorist events of 11th September 2001 (referred to as '9/11') brought the question of domestic security firmly into the purview of military ISR; this change complicated not only the technical issues but also, more importantly, the legislative protocols for sharing access to products and insights. Such legislative issues would benefit from further consideration, noting that progress has already been made in allocating policy responsibility to the Australian Geospatial-Intelligence Organisation (AGO) for adopting such whole-of-nation perspectives. AGO is now the whole-of-nation manager for all aspects

of the production, certification, and distribution of geospatial data for government and national purposes.

The recent setting up of the Australian Cyber Security Centre also provides a useful example of innovative policy approaches to new and evolving national security challenges. The Australian Federal Police (AFP) provides a good example of tactical sharing of information with other law enforcement agencies, such as the Australian Crime Commission and State police, and could serve as a model for closer cooperation across government and across the nation.

As Australia pursues greater integration of ISR, it will need to better define the roles and contributions made by members of its national security community, and address that community's cultural challenges, including problems with cooperation that are exacerbated because of fiscal constraints, different technology (as well as different standards), and different legislation (with different agencies operating under different Acts).

Australia's ISR capability development mechanisms need to be better synchronised. There are different life-cycle durations for software, equipment, and platforms - in essence, they have different technology refresh cycles. Yet, they are shoe-horned into identical capability development processes that have evolved for the acquisition and sustainment of traditional major platforms. ***It is time to move away from a systems-engineering perspective for acquisition of ISR capability to a software-engineering approach that is better-suited to short life-cycle and software-dependent ISR capabilities***. Such a move would be better enabled through an established ISR Enterprise approach.

Australia's Chief Scientist has called Australia "the mendicant country" with respect to science, and this is most obvious in the nation's access to non-defence satellite data. This is particularly significant when considering the broader national security concerns. For example, the Black Saturday bushfires were tracked through China's National Space Administration; weather is predicted using Japanese satellites. Whenever Australia monitors crops or water supplies, it is giving valuable commercial and other intelligence to others.

The concern here really is about the degree of control that Australia has over the sources of data that inform national decision-making. Australia's ongoing reliance on foreign sources is a significant issue and one that will be difficult to address during this time of funding constraints, as it leads naturally to the need for some degree of indigenous capability. The question becomes one of balance between sovereign control, access and investment for ISR assets beyond those that form part of the traditional military security arrangements; and how to balance sovereignty and security in Australia's dealings with neighbours, allies and others.

It does seem that Australia's agencies have evolved an effective policy-coordinating mechanism at a national level; ***however, there remains a lack of synchronisation in funding, capability development and maintenance, and standard setting, which conspire against achieving a true national-level ISR capability***. This needs to be remedied.

FUTURE POLICY OBJECTIVES

While effort continues in improving Australian ISR organisations, the use of existing ISR capability, and in international and national ISR cooperation, much more is needed. As mentioned earlier, this Kokoda Foundation Study has identified four key policy approaches or objectives on which to focus for the future evolution of ISR – these are: adopting a whole-of-nation approach, improving public engagement, accelerating the data-to-decision cycle, and synchronising capabilities. These are discussed in more detail in the remainder of this Report.

Adopting a Whole-of-Nation Approach

One of the great successes of the last decade has been the recognition that Australia's national security challenges require a Whole-of-Government perspective to ensure greater coherence across federal government agencies. One manifestation of this approach has been a migration from a 'need to know' posture to one of a 'need to share'. As laudable as this move has been, it now needs to be extended to a Whole-of-Nation approach, to include

State-level agencies, as well as others in industry, academia and the broader community.

This call for an expansion of the evolving Whole-of-Government approach acknowledges that agencies will be wary of pushing too far too fast, and of formalising something that has been going on organically for some time and that seems to have been working effectively. Thus, it will be important for any change to be seen in the context of building on current successes. This needs to be set within the context of how the agencies have responded to new challenges that have arisen over the past decade, and might start with evolving the current levels of cooperation within Australia and with the United States.

Recent Developments Reflecting a Response to a Changing World

Events over the past thirteen years that started with the '9/11' terrorist attacks have led to tremendous change in the national security environment. This has included the perceived role and responsibilities of the intelligence community in Australia, resulting in a widening of scope of what the respective agencies do. The advent of the National Intelligence Coordination Committee (NICC) has resulted in different agencies now aggregating and reviewing how effort is being deployed to address that increase in activities.

Most recently, Australia has recognised the need for a better approach to cyber security by broadening the role of the Australian Signals Directorate (ASD) to embrace all of government, and as mentioned earlier, the Australian Geospatial-Intelligence Organisation (AGO) now has a wider responsibility for geospatial awareness. Transnational crime also provides an example of the response to environmental conditions that demand the formation of new relationships. Border protection is the latest example of this broader response to changing circumstances.

Notwithstanding these positive developments, there has been a tendency for Government and the policy organisations to expect additional activities to be taken on without other activities dropping

off the agenda. It is vital for the senior leadership of the country to understand and be engaged in the vast breadth of the intelligence business that reaches from tactical operations support to counter-terrorist and cyber activities to strategic functions and support to policy-makers. This understanding and engagement is needed to enable the senior leadership to help set priorities, which should also address the challenge of non-core work being carried out that can distract intelligence agencies from their core functions.

Evolving the Current Levels of Cooperation

Australian intelligence organisations have assisted each other in discrete areas that do not compromise their legislative obligations, not because it was part of their function to do so but because it was in the national interest. ***It is this sense of cooperation that must be harnessed to drive a new culture around closer collaboration in ISR more broadly that also brings in non-Commonwealth government organisations such as academia, industry and other civic actors. However, a more strategic design will be needed to ensure this enhanced collaboration across the ISR Enterprise***.

Australia's ISR community has gone through a decade of rapid growth and also rapidly rising expectations of it and increasing demands being placed on it. This is especially so in the intelligence community. However, in this current period of fiscal restraint, any unanticipated demands will prove difficult to manage. The challenge for the ISR community now is to demonstrate that it is meeting most of its obligations with what it has to hand, but that real improvements can be derived from a modest increase in resources and/or a re-prioritisation of activities.

The challenge for Government will be to recognise that ***increased investment will be needed to facilitate any move to a Whole-of-Nation ISR Enterprise that will, as it matures, deliver efficiencies***, particularly through rationalisation (and thus removal of duplication) and better integration of processes, people, technology, and administrative arrangements.

Funding

Funding needs to occur on a predictable basis for the intelligence community. Historically, certainly since the early 1990s, the intelligence community has experienced peaks and troughs amid increasing expectations, and, as a result, has tended to be somewhat disaster- or crisis-driven. ***This unpredictable level of funding must be eliminated and the process must become more systematic as these funding peaks and troughs also affect the quality and recruitment of analysts that, in turn, impacts negatively on the quality of the analysis itself***.

ISR collection needs to be enduring, established early and maintained as a strategic tool. Collection activities need to continue once the crisis is over. They need to be in-place and functioning before the next crisis occurs. Without this, results will not occur immediately due to the required lead-time to build capacity, no matter what the Government's urgency.

Working with the United States

With the increased focus on the Indo-Pacific, Australia has a wonderful opportunity to expand its partnering role with the United States in terms of ISR across the region, as well as in space and cyberspace. Australia's Over-The-Horizon Radar (OTHR), also known as Jindalee Operational Radar Network (JORN), is a crucial piece in this, with its ability to detect and locate aircraft, missiles and ships in monitoring sea lanes and maritime chokepoints to the north of Australia.

As has been suggested by US analysts, it might be possible for JORN to be upgraded to detect and track ballistic missile launches, stealth aircraft and cruise missiles. Furthermore, other regional countries could support receiver stations to extend JORN's coverage, and thus be part of a regional ISR capability.[3]

3 These ideas are raised in Jim Thomas, Zack Cooper and Iskander Rehman, 'Gateway to the Indo-Pacific: Australian Defense Strategy and the Future of the Australia-U.S. Alliance', Center for Strategic and Budgetary Assessments, 2013, p.21.

With the introduction of Airborne Early Warning and Control aircraft, the Hobart Class Air Warfare Destroyers, space-based sensors, High- and Medium-Altitude Long-Endurance maritime surveillance UAVs, and P-8A maritime patrol aircraft, there is real potential for Australia to integrate intelligence data from these platforms with that of JORN. Such a capability could be part of a shared capability with the United States for processing, exploiting and disseminating ISR information to enhance situational awareness in the Indo-Pacific.

There is also a possibility for Australia to support and extend the United States' ability to monitor space launches and track satellites.[4] The space situational awareness partnership, the stationing of a C-Band space surveillance radar, a space surveillance telescope, and a combined communications gateway for the Wideband Global Satellite constellation of communications satellites are all examples of closer current cooperation between Australia and the United States that can be built upon.

Strengthening Australian cyber and Electronic Warfare (EW) capabilities will contribute to a joint capability to disrupt hostile ISR and Command and Control (C2) systems during, or in the lead up to, conflict. As Ross Babbage suggests, Australia could undertake "sustained investment in high-grade cyber and information warfare capabilities for use both in protecting Australian and allied systems and also for infiltrating, disrupting, and/or damaging an opponent's critical command and control and other high-value electronic systems".[5]

Regional ISR Infrastructure

The absence of capabilities in key areas, particularly situational awareness in the maritime environment, continues to pose problems for national security decision-making. The choices that other nations make in the South China Sea will affect Australia's national interests,

4 Ibid, p.22.

5 Ross Babbage, 'Strategic Competition in the Western Pacific: An Australian Perspective', in Thomas G. Mahnken, Ed., *Competitive Strategies for the 21st Century: Theory, History and Practice*, Stanford University Press, Stanford CA, 2012, p.250.

but the understanding of the airspace and naval space by these nations is very limited. Australia immediately encounters problems when trying to transfer skills to help improve air and maritime awareness in regional countries. However, Australia could approach this slightly differently in future by ***developing best practice in the area of ISR infrastructure resilience and transferring this to benefit regional countries that are still in the early stages of developing and connecting their ISR infrastructure***.

Integrating the Elements of ISR

Any notion of integrating ISR in a strategic national sense and determining how best to synchronise and integrate the planning and operation of sensors, platforms, and Processing, Exploitation and Dissemination (PED) systems, demands a new focus on those elements that constitute the ISR function, such as:

- *Planning and Directing*. This involves determining integrated ISR requirements, developing appropriate integrated ISR architectures, preparing an integrated collection plan, and issuing orders and requests to information collection agencies and assets in an integrated fashion. This would enable the improved synchronisation and integration of collection, processing, exploitation, analysis, and dissemination activities and resources to meet information requirements of national strategic and operational decision-makers.
- *Collection*. Collection involves the acquisition of information and the provision of this information to processing elements. An integrated focus would provide the ability to obtain all of the required information to satisfy diverse ISR needs (through use of sources and methods across the entire ISR Enterprise). Collection activities span the full range of military, border protection and law enforcement operations.
- *Processing and Exploitation*. Processing and exploitation involves the conversion of collected information into forms suitable to the production of intelligence. An integrated focus would provide the ability, across the full range of military, border protection and law enforcement operations, to transform, extract, and make available collected information suitable for further analysis or action.

- *Analysis and Production*. Analysis and production involves the conversion of processed information into intelligence through the integration, evaluation, analysis, and interpretation of all source data and the preparation of ISR products in support of known or anticipated user requirements. An integrated focus would provide the ability to better synchronise, evaluate, and interpret information from all available sources to create a mature ISR product that addresses a multiplicity of perspectives for presentation or dissemination to enable increased situational awareness across the full breadth of users.
- *Dissemination and Integration*. This involves the delivery of ISR product to users in a suitable form and the application of the product to appropriate missions, tasks, and functions. An integrated focus would provide the ability to present information and ISR products across the full range of military, border protection and law enforcement operations enabling understanding of the operational environment by the relevant decision-makers.

Improving Public Engagement

How Intelligence Works

Intelligence is not just expected to provide answers; it is expected to prevent surprise. Accordingly, most of the intelligence community's work is not in response to specific questions asked by policy-makers; rather, the intelligence agencies have to be seeking new information and new insights about new topics that might loom as problems in the future, while also addressing current requirements.

Intelligence agencies conduct their intelligence collection and analysis operations according to a rigorous and well-established system, and policy-makers participate fully in that system. The intelligence agencies also operate strictly within the limits set by legal statutes and other administrative instructions.

In relation to the Edward Snowden revelations and implications for Australia, Prime Minister Abbott expressed his confidence in early

December 2013 that Australian intelligence agencies were acting within the law and that there were proper safeguards. The Attorney-General, Senator George Brandis, also pointed out in December 2013 that surveillance by Australian agencies was governed by a strong and sound legal framework that provided an appropriate balance between national security and the right of citizens to privacy. The Attorney-General was at pains to highlight that Australia's intelligence activities and its intelligence agencies were designed to serve Australia's national interests and protect Australian citizens.

Reporting also indicated that neither the Australian Signals Directorate (ASD) nor the Australian Security Intelligence Organisation (ASIO) collects or shares metadata in bulk. Some specific metadata is shared in investigations involving overseas agencies but ASIO's metadata collection is in line with ministerial instructions and subject to internal checks. While ASIO does not require a warrant to access the information from a telecommunications company, it would require a warrant from the Attorney-General if it wanted to investigate the actual content.

ASD collects only specific foreign intelligence metadata. ASD can access information on Australian citizens if it has a ministerial authorisation, which would have to be signed off by the Attorney-General. Authorisations have been granted in the past in relation to communications between terrorist organisations and Australians.

It is important to note that Australia's intelligence agencies are overseen by the Inspector-General of Intelligence and Security (IGIS) and a federal parliamentary committee. IGIS staff have visibility of the activities of the intelligence agencies and are briefed regularly on sensitive operations, receive intelligence product, have access to systems, and carry out regular inspections of activities.

It is the contention in this Paper that the current intelligence community is performing within the expectations of the Government and that the internal focus of intelligence needs to remain within its current framework, which means that the public and the Government have a social compact that limits the Government's ability to spy on or to control its citizens. ***In developing a sovereign ISR capability for protecting national borders and beyond, the Government needs***

to focus on areas of national interest that do not compromise the rights, privileges and privacy of its citizens.

The IGIS role represents a strong institutional advantage as it is a focal point for ensuring accountability and it delivers to the public a sense of confidence that the intelligence community is doing the right thing. Thus, ***the IGIS position could be used more in improving engagement with the wider public and in improving the sense of trust that exists in the ADF***. This could be further expanded upon through greater collaboration with the Privacy Commissioner. Furthermore, the IGIS role could be extended to ensure that a national surveillance asset was only used in support of an ISR mission or task, with its focus on sovereign or military interest. In this way, the IGIS could ensure that the ISR community's missions and tasks were not infringing citizens' rights.

Social Licence

There is a gap between the requirements of the national security function and the popular expectations in Australia when such functions are perceived as affecting privacy and personal freedoms. As was evidenced after '9/11', the broader community can sometimes grant a social licence for measures that might be seen as breaching privacy or personal freedoms; however, as such crises become dimmer in society's collective memory, the social licence can be withdrawn. Consequently, measures such as those required to retain telecommunications data, for example, can be denied.

Acceptance in society of the intelligence community and its need to have a particular set of powers – the granting of a social licence - will tend to be predicated on a level of transparency about what the intelligence community does domestically and improved understanding by society. ***Public fears around the invasion of privacy need to be allayed, which demands greater transparency from the Government and public officials. But it is more than transparency as the public can also act as a resource; thus greater engagement with the public is needed***.

Unmanned systems are a good example of the lack of understanding and concern within the general community. Unmanned systems can

deliver a significant level of national self-reliance for ISR, as well as make a valuable contribution to regional cooperation. Unmanned systems can contribute to humanitarian assistance and disaster relief, border surveillance, cargo delivery, medical evacuation, hydrographic and geographic mapping, and climate analysis can be made at very short notice, providing immense value to regional neighbours with limited ISR resources. The autonomy of unmanned systems needs to be set within the context of positive control by humans who have certain responsibilities around how these vehicles are used – so it is important for this information to be relayed to the public.

Because of this lack of public discourse involving the intelligence agencies and the public, and more importantly, the role of intelligence collection in the ISR Enterprise, the ISR community and the agencies have not been very adept at responding to tactical shocks. They inevitably end up on the back foot when things go wrong. Thus, it is incumbent on the ISR Enterprise to be more accessible to the public - to be an audible voice and to be visible, transparent and accountable. In this way, the public can also take a more active role in the national ISR construct and better understand how each organisation within the ISR community contributes to the overall Enterprise.

Improved communication must be part of the strategic dialogue between Government and its key departments, the ISR Enterprise and the public. By informing people about checks and balances of the ISR Enterprise and its responsibilities, Government can substantially increase the level of trust from the public; thus providing support even when uncomfortable issues arise. It is in Government's interest to encourage the ISR Enterprise (and specifically the intelligence institutions) to be more publicly engaged, and indeed for Government to more actively support them in this.

Accelerating the Data-to-Decision Cycle

The advent of computing has seen a meteoric rise in the amount of information that is generated and stored about the environment in which the world population lives and functions. Organisations and Governments across the world are seeking ways and means to exploit the information collected for political, economic, military and personal gain.

In the military and national interest sphere, the use of this data provides the potential to develop an understanding of events and connections that might otherwise be invisible. The private sector has exploited this data explosion to understand buying behaviour and the behaviour of competitors. Similarly, governments have collected significant volumes of data through Signals Intelligence (SIGINT). Compared with the private sector and intelligence community, military and law enforcement forces have adopted a very modest approach to exploiting this abundance of data, which is referred to as 'Big Data'.

Big Data

Big Data does not just encompass volume; it also addresses variety, velocity and variable veracity. These are the characteristics of Big Data, but the issue is also about the relationships between these characteristics and how an organisation manages and exploits these relationships.

The United Kingdom's Ministry of Defence's vision for Big Data is one that brings together all the necessary data and exploits it so as "to establish clarity, increase efficiency and gain previously hidden intelligence". Thus, users will be able "to access and analyse timely and trusted information from the most appropriate sources, through a variety of interfaces".[6] The opportunity that Big Data affords Australia is to discover the hidden intelligence through the harnessing of sensor data in a meaningful way. Australia probably has all the data it needs today, but does not have the wherewithal to bring it all together to make a difference.

It is worth noting that Big Data analysis systems have been implemented in other countries, which in the case of the United Kingdom, notwithstanding the initial expense, saw the customs system pay for itself in the first year of operation through increased customs revenue. New Zealand has embarked on a similar system. It is also worth noting that the increased revenue side of the equation

6 See Network Technical Authority, 'Big Data: A NTA Technical Vision, Rev, 0.4', DE&S Information Systems and Services, 1 August 2013, p.5.

is complemented by a 'safer borders' benefit. These anecdotal comments were provided during research for this Project, and it would be useful for government officials to pursue the veracity of these claims and capture any relevant lessons learned.

Ultimately, Big Data is about how the data is stored and managed and then how it is shared – and, in the final analysis, how it gets to the decision-makers. However, this desire to share data still has to overcome some legal roadblocks and technological and cultural problems.[7] Since this is where Australia is heading, it should not be left to happenstance for these sorts of problems to be resolved; rather, ***a plan is needed to get there*** and to ensure legacy problems and privacy concerns do not become show-stoppers.

Many of the structural and systemic limitations of the past, such as incomplete data sets and lack of analytical capabilities, (which restricted the ability of organisations to gain fuller insights from the data collected) are now being overcome through the ever-increasing volume, variety and velocity of data, and the commercial sector's technological and analytic capability to smartly mine this data.

The ISR Enterprise can learn from how successful businesses have used Big Data to improve their competitive advantage through meeting three challenges. The first challenge is to identify the information and how and where it is stored. The second challenge is to tag the data to allow its characteristics to be identified. The third challenge is to run the data through an algorithm that allows it to be collated and presented to an analyst. By overcoming these challenges, the ISR Enterprise can use Big Data to help make better and faster decisions.

Australia has relied on the United States as the dominant source of ISR capability (for example, US satellite technology underpins much of Australia's imagery capability and spatial awareness (location)). ***It is quite likely that competence and capability in Big Data will become a mandatory requirement for future operations with***

7 The quasi separation of military and law enforcement powers is one example, where military assistance has to be formally requested for disaster relief.

the United States – and Australia will need to address this if it wishes to continue to access US ISR capability in future.

Analytics

ISR data comes from a number of sources and platforms, and is quite diverse, with large quantities of imagery and video generated every day. ***Big Data analytics have a potentially significant role in helping to manage the flood of data and assisting analysts to focus their efforts on analysing content rather than searching for relevant information***, while also ensuring full adherence to laws and regulations that protect citizens' rights. Big Data also has applications in cyber security, providing network managers with the means to process large numbers of attacks and identify the more serious advanced persistent threats.

The ever increasing volume and velocity of data means greater emphasis is needed on analytical capability and greater protection is needed for analytical integrity. The data is out there somewhere, and the real issue is accessing it and working through it meaningfully in a time frame that allows the true value to be derived. While infrastructure is key, so too are agile commercial relationships that will help reduce the cost of operational maintenance and allow investment in enablers as well as the traditional platforms and sensors.

The impact of failing to exploit national security-related data could be far higher than that faced by the private sector which has to deal with loss of profit or market share. The operators expect rapid intelligence to support their responses, with timeframes measured in seconds, which demands constant and rapid analysis. Intelligence analysts are moving away from monitoring routine 'pattern of life' details to immediate analysis of fleeting, real-time data. ***This demands corresponding improvements in tools and techniques to support the search and analysis of data***.

Automated analysis technology is the top ISR priority for many practitioners. They are concerned over any imbalance between investment in collectors and in the tools to support analysis that takes into account all available sources in the assessment. Algorithms are needed to allow analysts to perform real analysis. It is vital to develop

capabilities that dramatically improve the ability to manage and use the data. AGO has started down this path and adopted Big Data techniques to help analysts sift through satellite imagery and monitor changes in areas of interest around the world.

As John Edwards[8] has commented, there is little trouble in aggregating the massive amounts of data but putting all of that to productive use is another story. Big Data tools have now become essential for sorting through and making sense out of these massive and growing amounts of data. But just as important is the ability of the ISR Enterprise to continually update and augment its analytical capabilities, which means the solutions must be able to scale. Furthermore, as the community also has great need for speed and agility in its solutions, so open source software becomes a key requirement.

Those ISR organisations that will benefit most from Big Data are the ones that rely on detailed analytics - signals intelligence, electronic intelligence, and human intelligence - as well as those which use substantial amounts of data to underpin their products, such as the AGO.

These organisations will need to add to their teams, people with an advanced background in statistics, data mining and machine learning skills. Such people will be crucial in getting the most out of various technological innovations and tuning them to the particular needs of their organisations. Machine speed and processing power, as important as they are, can never be a substitute for human creativity and intuition at the level of complexity and abstraction that will pertain.

The potential benefits of Big Data analytics are significant but need to be approached with an awareness of the associated risks and challenges, especially in balancing the need to protect information with the potential benefits of sharing. Currently, this balance does not seem to exist and the barriers to sharing are too high. Big Data will not solve this. So, ***there is a need to develop a culture, supported by corresponding policies, that incentivises data sharing for the***

8 John Edwards, 'To tame Big Data, intelligence community needs tools that scale', *C4ISR & Networks*, 12 November 2013.

greater good as well as more sophisticated risk-assessment models and techniques around the sharing of data. By embracing an ISR Enterprise approach, rather than encouraging independent and individual entities, such a culture could be developed and enhanced for Australia.

Societal Context

There is a societal context that needs to be addressed as the collection, transmission and use of volumes and variety of data today are larger by orders of magnitude than has historically been the case. The exponential growth in the volume of data needing effective management is a function of the growth of the internet (particularly social media) and more capable sensors in both commercial and military systems that create and distribute much richer data for eventual analysis.

Social media conversations and themes will need to be factored in to any solution. And these will have greater influence in humanitarian issues. Social media research is emerging as a practice that is conducted across the public, private and academic sectors. However, ***Social Media Intelligence (SOCMINT) is not yet a coherent academic discipline or distinctive intelligence tradecraft,[9] and needs to be developed as such***.

The Australian Government also needs to work in collaboration with data management and social media companies to improve Australia's national privacy principles and to establish guidelines that will strike a balance between privacy rights, security and commercial interests. Guidelines are needed that will help improve mechanisms for establishing accountability towards principles that help to protect and promote Australian privacy rights in a digital age.

9 See Jamie Bartlett and Carl Miller, 'The State of the Art: A Literature Review of Social Media Intelligence Capabilities for Counter-Terrorism', The Centre for the Analysis of Social Media, Demos, November 2013.

Skills

There is also a pressing need to address how the necessary data management and exploitation skills will be recruited, developed and retained, which will demand innovative collaborative partnerships with the private sector. Furthermore, a collaborative approach with the commercial sector that allows Defence to benefit from cutting-edge skills, possibly maintained in the reserve forces for example, merits investigation.

An Enterprise Architecture Approach

Australia needs to adopt an 'enterprise architecture' approach that allows, from a technical perspective, the removal of proprietary interests (standards, protocols, etc) that affect interoperability, and the removal of obstacles imposed through stove-piped acquisitions. These all constrain the evolution of a sovereign ISR capability.

During research for this Paper, the current situation was described pithily as 'shoeboxes of data of uncertain provenance, managed under inconsistent policies for metadata standards, storage or retrieval'. These legacy problems will continue without an overarching strategic plan and statements of intent to align. This includes the need to design and adopt an architectural approach, with clear rules about sharing specific data, noting that not all data is shareable to all in the ISR Enterprise. Furthermore, there is no point in trying to connect databases that are not designed for connectivity.

The Defence Chief Information Officer Group (CIOG) 2009 ICT strategy should yield an enterprise ICT structure upon which a Defence ISR capability can be delivered. However, this needs more support and acceleration if it is to meet its initial capability by 2016 and full capability by 2021. Achievement of such a strategic, consolidated construct within Defence could then be used as a base for expansion across Government, and, ultimately, across the nation.

A substantial body of work is being done by disparate areas, and it is being brought together nationally. The National Security Advisor's

Roadmap out to 2020[10] shows the clear policy intent for improved IT alignment across agencies, and, while implementation problems still exist, they are not insurmountable.

An enterprise-level architectural approach would also help Australia understand its national processes and data flows to ensure that human judgment is applied and that legislative and regulatory requirements are observed. Access control and authentication algorithms that dynamically limit user permissions to correspond with changes to the sensitivity of merged datasets will be necessary, as will an awareness of where information is held, the jurisdiction that applies, and the legal obligations and freedoms that implies. One positive development is the implementation of attribute-based authentication, in which the data has a privilege and not the user.

Data Responsibility

The architectural approach would also help in managing the provenance of data. For example, while the volume and other aspects of Big Data can be dealt with technically, the current challenge is the data responsibility spectrum. At one end, AGO is responsible for handheld data, but at the other end, AGO/AGD (Attorney-General's Department) are responsible for high-grade classified data; however, there is a lot in between, ranging from base cameras to interrogation cameras. This is tedious work in some respects, but it is not well understood or acknowledged as an issue. Indeed, it is probably the subtext of the data-to-decision topic for ISR – the provenance of the data, the responsibility for the data, and getting the data to the decision-makers.

Approvals Process

Adopting an enterprise architecture approach and leveraging developments in Big Data can help to better synchronise ISR technology. However, they will not resolve challenges posed

10 Department of the Prime Minister and Cabinet, *National Security Information Environment Roadmap: 2020 Vision*, 2010.

by the approvals process, which needs some serious overhaul, particularly because technology is moving so fast. The tradition of creating monolithic projects that set requirements years out from implementation is not defensible for short life-cycle and software-dependent ISR capabilities. ***A program-centric approach within an enterprise architecture is needed, supported by faster project cycle times and evolutionary acquisition*** as a matter of course.

Fifth Generation Capabilities

The price of entry into the ISR community is now very high, and in order for Australia to sustain its current access, a more strategic approach is needed, along with a substantial degree of culture change. The United States has invested enormous amounts of money in transitioning to its current capability. Geospatial data is now provided for appropriate projects, with planners having realised just how much data is required in projects. The F-35 Joint Strike Fighter (JSF) project representatives and representatives from the intelligence agencies communicate in order to determine the overall intelligence data requirement to ensure project success. In Australia, intelligence has not been sufficiently recognised as a fundamental component of military capability.

The JSF will ingest data and deliver data in significant volumes - data which will be of significant value to Australian interests. Australia is only now starting to grasp what this fully means and the extent of change needed for the ISR Enterprise to best support this capability. Defence is setting up areas for looking beyond the JSF and how that data will be delivered and in what form. This is a new challenge for Defence and one Australia has not had to face until now. The new fifth-generation capabilities such as the JSF and Air Warfare Destroyer will bring profound changes to the ISR Enterprise around data management and data security, and Australia needs to start planning for those changes now.

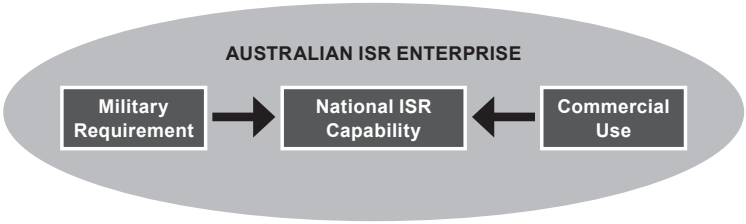
Synchronising Capabilities

A multi-disciplinary approach to ISR is needed – collection capabilities must complement each other and any limitations in one

system should be able to be mitigated through capabilities in other systems. A multiplicity of sensors, sources, systems and techniques is needed, ensuring that a diversity of insights can be provided by different assets to ensure the fullest understanding of the situation. These ISR assets are becoming increasingly important, not only to support operations, but also in becoming an intrinsic part of them, and therefore need to be secure. Furthermore, complete understanding of the situation can only come through a clear presentation of the fusion of these insights from different assets, which will help ensure effective decision-making and proper and prompt responses.

While much of the concern over cyber security today focuses on Internet-connected networks, the ISR Enterprise also faces challenges around its non-Internet-connected networks, such as tactical data links and satellite-control networks. Future warfare will involve these types of networks and the systems that connect through them, such as satellites, avionics, targeting pods, digital radios, and unmanned systems. Effects produced on and through these systems will include disruption, distraction, distortion, distrust, confusion, and chaos of both a virtual and physical nature. Operators will need to address defensive hardening and attack recovery across all networks – both those connected to the Internet and those not traditionally based on Internet data-transfer protocols and technologies.

The landscape is characterised by the need for a national ISR capability, with the military requirement at one end of the spectrum and commercial use at the other end, as depicted in the Figure below. There is no question that ASD and AGO will now have the responsibility of providing information to the State governments – so in a sense, Australia is already moving towards a whole-of-nation approach. But are the capabilities being effectively synchronised?



The Stove-Piped Focus on Projects

There is currently a problem with some projects already in the pipeline in terms of how their geospatial data requirements can be satisfactorily addressed. At the pre-First Pass stage of the Defence requirements process for example, ***there needs to be greater recognition of the importance of joint force integration and the need for innovation***. Australia needs to move quickly through addressing its Defence legacy data and systems, and involve other industries in helping to address the future integration challenges. However, this needs the right level of funding, the strategic vision and intent, and a clear set of national requirements.

JP2096 will provide the backbone for ISR integration (but it is unlikely to address sensor integration). First Pass is not scheduled until June 2014. Furthermore, JP2096 is the responsibility of the Chief Information Officer Group (CIOG), presumably to ensure compatible communication standards across Defence, but it lacks a definitive capability manager who, as the business process owner, would provide the business architecture. Functionally, this Project should provide the 'glue' – bringing together the platforms, sensors, data and human decision-makers. Planning for platform sensor integration is important and should be part of JP2096 for all future Defence Capability Plan projects. For example, plans are needed for transferring the ISR product that will be captured by the P-8A Poseidon aircraft to the ISR Enterprise.

JP2064 (referred to as the smart map) will provide the geospatial piece (but phases 2 and 3 are yet to clear First Pass)[11] while JP2044 will provide the intelligence piece (Phases 4a and 4b, but how will the project come to market – a sensible industry approach would have been for a $40m program but it is likely to come out as 10 x $4m programs). It does appear, however, that this Project, also with CIOG, has at least adopted an evolutionary acquisition approach.

11 JP2064 Phase 2 is the basic geo-portal, while Phase 3 is the geospatial infrastructure, information, and services. This project should be accelerated, with all phases being better integrated.

JP1770 (maritime rapid environmental assessment that uses the amphibious capability to move forces to the beach) and JP1771 (that moves the forces onto land – Army geospatial support systems) have yet to address how to get the data off the assets and into ground stations. Air Force has three small $5m projects looking at this. JP1778 is another related project that deals with mine countermeasures and concentrates on the area close to the lodgement. RPDE Tasks 49 and 50 are looking at how geospatial data is to be used to inform SEA1430 Phase 8.

There is also JP2065 Phases 1 and 2 – Integrated Broadcast Service – which is based around a US satellite UHF communications system, and JP2044 Phase 4 – Digital Topographic Systems upgrade.

So, with all of these projects running, is there an understanding around who owns ISR in Defence and who ensures the information is passed to the ADF and to the wider national security community? There is a lot of ISR architecture work still needed, which probably needs to be done by the Integrated Capability Development Branch of Capability Systems Division in Defence. Perhaps it is time to re-think the Defence structure and ***make one of the Defence Joint three-star military officers responsible for Defence ISR, and one of the deputy secretaries in the Department of the Prime Minister and Cabinet responsible for policy coordination across the national ISR Enterprise***.

The nation needs an all-source ISR capability but that takes time and Australia cannot really wait 10 years for this to emerge. Should there be a two-star ISR Command to speed things up, or as mentioned above, appointment of a Defence ISR Capability Manager? Australia's ISR capability has tended to focus on the nation's strategic defensive posture rather than its deployed military posture, which must change. There is a predictive strategic element of ISR which is not done well, and there are tactical elements that are managed well. Would a two-star ISR Command or a three-star Capability Manager resolve this dichotomy? How does Australia merge its JORN capability with maritime situational awareness offshore and awareness in the airspace over major cities?

Clearly, there are dominant roles within Defence for Joint Capability Coordination Division (in developing concepts and policy), Capability Systems Division (in effecting program management), and Joint Operations Command (in using the assets and in helping to set the operational requirements). However, there are also integrative issues involving the various capability managers in raising and training their ISR forces, and in the acquisition and through-life support (or sustainment) of the platforms and sensors themselves. Notwithstanding these observations for improved coordination and integration, it is also vital for the professional mastery within specific domains to be retained.

Supporting Deployed Forces

ISR can be a game-changer in the region. However, any real ***ISR capability needs to be connected to the US Pacific Command (PACOM) and the US Marines in Darwin. There really does need to be a dialogue on deployed forces and their ISR requirements***. Australian military forces have returned from the Middle East Area of Operations (MEAO) to an ISR 'steam age'. Australia has, for some time now, been working with coalition partners in deployed locations but that is now changing to simply being allies again. Australia needs a dialogue on future posture around its interaction with the United States – such as with PACOM.

Any dialogue on deployed force requirements also needs to address responsibility for deployed systems. For example, JP2072 – Battlespace Communications – is the responsibility of Army (with input from Air Force), but that shifts to the Chief of Joint Operations when forces deploy on an operation. Meanwhile, Navy uses SEA1442 to address its battlespace communications requirements. Furthermore, JP2072 will not be able to move all of the communications required for ISR, so future communications choke points will have to be addressed through JP2064.

This communications capacity issue will be exacerbated when tele-medicine starts being used extensively in supporting the deployed war-fighter. There will never be sufficient communications capacity to support all of the requirements. Thus, commanders

and other decision-makers will need to be clear as to what can be realistically delivered.

Evolution of ISR Capability

The evolution of ISR capability will become even more important as ISR exchange increasingly becomes a two-way process. The ability of the commander to ask for what can be practically delivered rather than depend on what is delivered because that is all that is available will become critical in future. This two-way process involves a deeper understanding of the agency that is tasking the ISR assets, of data/information fusion, of intelligence analysis, and of the capabilities and limitations of the processes and systems, all of which leads to more-informed tasking. This would make for a more efficient and effective use of the end-to-end system intended to improve or enhance knowledge of the battlespace for the military, or the operational space, in the case of law enforcement.

It is important for ***Defence ISR to improve engagement with the capability managers; to adopt a program approach to capability development for ISR; to bring industry in as an integral part of the capability development process and ensure industry aspects are considered early, appropriately and consistently; and to make better use of the Capability and Technology Demonstrator (CTD) and Rapid Prototype Development and Evaluation (RPDE) programs***.

The ADF is facing a change in the nature of its operations through the diffusion of threats, global communications, and the increased use of unmanned systems, all of which place new demands on the ISR Enterprise. The increase in low-intensity insurgencies and international criminal organisations has blurred the lines between combatants, criminals, and non-combatants. It is important to better understand the use of force as it relates to unmanned systems, and create a suitable social construct for their use that is more conducive to national security policy than the negative connotation that has built up over recent years. Australia needs to formulate a national policy for unmanned systems and a social construct that will support the platform rather than hinder its utility.

In developing its thinking about ubiquitous ISR, Australia should note recent comments from retired US Air Force Lieutenant General Garry Trexler.[12] Trexler argues that the growth in the military's demand for ISR continues unabated, exacerbated by combat forces bringing their own tactical ISR platforms with them into the Area of Operations, to improve responsiveness and reduce dependence on others, including national systems. Trexler argues for a more resilient overhead persistent infrared architecture than a wide-field-of-view approach offers based on third-generation infrared surveillance technology.

Trexler also argues for improved Mission Data Processing, noting that identifying intelligence Processing, Exploitation and Dissemination (PED) tools for the future is no easy task.[13] His answer to coping with an expanding amount of imagery is to continue to improve the software, expand automated processing, and provide more sophisticated workstations for analysts. However, he argues for greater focus on the people side of things - recruiting, training, and retaining sharp, capable people who are able to deal with the modern-day challenge that is going to become even more complicated.

Trexler's suggestion about embracing new fifth-generation capabilities in a formal ISR role, indicates the need for Australia to think carefully as its fifth-generation capabilities are introduced into service. Government and military commanders will need to state their requirements in conjunction with advice from the ISR community on what is feasible and at what cost. Assignment of priorities to particular information and intelligence requirements will also need to be a cooperative determination.

Requirements will also have to be balanced with cost and technical feasibility. Taking the JSF as an example, its sensor suite could generate terabytes of data, which would be far more than could

12 Lieutenant General Garry Trexler (USAF, ret'd), 'Space: Tomorrow and Beyond', in *Strategic Studies Quarterly*, Vol 7, No 3, Fall 2013.

13 A range of current projects, including JP2064 and JP2044, are PED-related and urgency to bring them to Initial Operating Capability has been recognised. PED tools are critical in better synchronising capabilities.

possibly be recorded, much less down-linked, in real-time. Therefore, precision in the exact requirements of users will need to be provided and understood by the ISR community.

Further questions concerning the nature of the data will need to be asked – for example, will raw data suffice, will fused data used by the operators be enough, will other analysis and insights be needed to support more strategic decision-making? Commanders are already demanding access to unprocessed data because of the delays associated with processing. The real concern is to only supply data which a Commander can use. Thus, there is the need to 'push' critical data/intelligence as well as allowing 'pulling' from central databases. It is understood that the United States National Reconnaissance Office is pursuing this model.

ISR capabilities of unmanned systems such as the MQ-1 Predator and MQ-9 Reaper in Iraq and Afghanistan have resulted in a transformation of ISR from a support tool to a vital part of every military operation for the United States. Australia too is moving along this transformational path through its experience with Heron and Shadow UAVs.[14] Transformation is occurring on another related front as well with the target-based, inductive approach to ISR transitioning to a problem-based, deductive and proactive anticipatory approach.

There is also a conflation of cyber, space, Electronic Warfare and ISR that all need to be integrated into a holistic ISR picture – often referred to as 'fusion'. Institutional barriers and outdated administrative arrangements need to be removed and ISR capability synchronised and consolidated into a national effort. While synchronising platforms and sensors would be a good start-point, that synchronisation must extend to professionalising the analytical workforce and investing in automated technologies.

14 For an excellent discussion on future directions for Australia's Unmanned Aerial Systems see Williams Foundation, 'Protecting Australia with UAS', February 2014.

United States Developments

The United States is using ISR in different environments in different ways and different companies are at the heart of the solutions, particularly in supporting the Army, the Air Force, the Navy, and the intelligence community. The United States is addressing integration of its backbone systems and Australia needs to capitalise on these efforts.

The US National Reconnaissance Office has established a standards framework (Defense Intelligence Information Enterprise (DI2E)) that is focussed on the promotion of Distributed Common Ground Station (DCGS) interoperability through either technology convergence, or federation. There is a strong desire for coalition integration at the ISR/DCGS level which indicates that adoption of the DI2E framework (with a limited but suitable adaptation to Australian conditions) would be pragmatic.

Australia will need to leverage the lessons learned by the United States in its rapid build-up of its separate, Service-centric DCGS networks. As a consequence, the United States has had to develop the DCGS Integrated Backbone (the DI2E set of data-sharing servers and standards) at considerable cost and time to link the various DCGS systems together so analysts can share information. In its Defence ISR Integration Backbone, Australia is seeking to start with an overarching, or enterprise, approach to intelligence collaboration, which equates with the US DI2E framework.

Noting that Australia will seek a multi-source/multi-Service/multi-theatre ISR capability, one option that should be explored is the forthcoming United States Marine Corps (USMC) DCGS. DCGS-MC may prove to be highly relevant to Australia's ISR posture due in the main to the USMC tri-Service structural similarity to the ADF and the desire to have a single DCGS capability.

DCGS-Intelligence Community has been identified in the United States as an exemplar in terms of the advantages it offers and should also be examined for whole-of-nation applicability by Australia. DCGS-IC is designed to serve the US national intelligence agencies and tactical DCGS military units by providing decision-makers, intelligence analysts and war-fighters with access to a variety of authoritative

data sources from across the national and tactical communities. The system draws upon data sources at the agencies and the military services, including those linked by other DCGS systems. Searches that formerly took hours can now be done within minutes.

PED is a very important ISR capability element in the United States that, notwithstanding improvements, still remains a deficiency in Australia's ISR arsenal. ***A mature PED capability would allow Australia to equip teams of analysts with software tools and give them the ability to share their products with other analysts over the network provided by the ISR Integrated Backbone***.

CONCLUDING COMMENT

Future ISR for Australia is about synergy. Integration and synchronisation allow the effects of collective ISR to be well in excess of their potential when they are separated. All of the data and information required for the production of *intelligence* are the result of *reconnaissance* and *surveillance* collection; conversely, the sole purpose of *surveillance* and *reconnaissance* is to collect data and information for the production of *intelligence*. The data collected depends upon processing and exploitation common to all three activities. Decision-makers tend not to be overly concerned about who provides the intelligence and how it is delivered. They are not asking for separate 'I', 'S' and 'R' streams on different displays or in different formats — they are expecting integrated products on identical timelines.

The complexity, ambiguity, dangers and speed of the emerging 21st century world require profound improvements in intelligence to detect problems as they arise and in networked response options to achieve the overall effect required. Faster and more complex operations and activities require deeper analysis and planning. Because of globalisation and the agility and interrelated nature of possible threats, the ISR Enterprise has to be comprehensive and address all sources and diversity of requirements, while also including both long-term and immediate-term analysis.

ISR must be treated as an integrated process, moving it in complexity, speed, and effectiveness beyond the current model of inter-agency cooperation. Indeed, cooperation, coordination and interoperability are no longer enough. Close collaboration is needed, which demands greater use of standards for integration and information sharing across all levels of government and beyond.

The ISR community is now undertaking a much broader range of functions across increased areas than in the past, which means new capabilities are required and a coordinated ISR Enterprise is needed to enable this additional work to be accomplished. All efforts need to come together in a whole-of-nation approach that brings in industry, academia, State jurisdictions and Federal agencies. This demands a strategic design from the outset, together with a new culture around closer collaboration. In addition, more effective management of scarce skills is called for at a national level. Resources will clearly be an issue, but just as importantly, Government will need to set national priorities.

This whole-of-nation question must start with the principle that ISR and its community represent a national enterprise-level capability. Forward planning is important for matching ends, ways and means, but it is increasingly vital for that planning to address unforeseen operational and strategic demands, and that requires a much stronger analytical capability and much closer collaboration.

It is vital for public engagement to be improved - the social balance between expectations of actions for security and the need for privacy must be struck if the ISR community expects to retain any form of social licence. Greater transparency of the checks and balances imposed on the ISR Enterprise can lead to a substantial increase in the level of trust from the public. It is incumbent on Government to encourage the ISR Enterprise (and specifically the intelligence institutions) to be more publicly engaged, and indeed for Government to more actively support them in this.

It is also vital to accelerate the data-to-decision cycle by adopting a Big Data approach which would allow Australia to deal with the increasing volume of data, as well as its variety, velocity and variable veracity to extract greater insights and more reliable prediction of

events. Such an approach can offer faster transition from collection to analysis, decision and action; and greater confidence in the analysis, decisions and actions.

It is crucial to develop the right capabilities for ISR and ensure they are synchronised, which demands from the start, a multi-disciplinary approach. Defence has a number of ISR projects in-train, but there is no single person in Defence responsible and accountable for ISR. Furthermore, there is no single person at the national level to ensure that Defence projects align with national requirements.

ISR can be a game-changer in the region but Australia's capability must be integrated with that of the Americans. Deployed force requirements still need a lot of work. The future deployment of unmanned systems in support of national security must also address the social context and considerable work is required in improving the public's understanding of the role of unmanned systems.

Noting that Australia will seek a multi-source/multi-Service/multi-theatre ISR capability, Australia should look to the forthcoming United States Marine Corps DCGS and the DCGS currently used by the US intelligence community. DCGS-MC might prove to be relevant to Australia's ISR posture due to the USMC tri-Service structural similarity to the ADF, and DCGS-IC is regarded by many as the exemplar for effective collaboration across diverse organisations.

From a strategic design perspective, Australia needs to align its vision, governance, infrastructure, data, and workforce across the ISR Enterprise. The start point is vision - in operational, technological and policy terms. Governance embodies shared understanding, shared commitment, and shared capability objectives, all of which demand close and effective cooperation, collaboration and trust across all agencies, their enterprise processes, their administrative arrangements, and their industry partners.

New information technologies have led to new network organisations, new types of collaborative communities and new demands being placed on government. Joseph Nye's interpretation of all of this is that information will be dispersed widely, power will

thus be distributed more widely and informal networks will prevail over traditional bureaucratic forms of communication. [15]

In examining the challenges that new information technologies are imposing on organisations, Nye also discusses the "paradox of plenty"[16] by suggesting that an abundance of information leads to a paucity of attention. As Nye suggests, when decision-makers are overwhelmed with the volume of information before them, they find it difficult to know what to focus on and their ability to pay attention becomes the scarce resource, rather than the information itself. This is, of course, exacerbated by the vast amount of free information that inundates them.

The ability to store data is falling further behind the ability to process it.[17] The key challenges of this for ISR include: storing the large volumes of streaming data from unmanned systems; accommodating the large volumes of unstructured data; and scaling up human analysts to deal with these increased data volumes. Moving analysts from being reactive to predictive and proactive, and automating the identification of risks and anomalies will be vital in this respect.

Innovation will be key for the ISR Enterprise to survive and thrive in the coming decades. And integration will be crucial, which itself introduces the unnatural act of sharing and using the knowledge of others to manage critical incidents. Enabling information sharing across government in this way would force collaboration and distributed decision-making to occur!

Interoperability and integration across agencies, governments and other third parties is costly and requires a commitment to the development of standards to which all agencies and all levels of

15 Joseph S. Nye Jr, *Power in the Global Information Age: From Realism to Globalization*, Routledge, Taylor and Francis Group, London and New York, 2004, p.82.

16 Herbert A. Simon, 'Information 101: It's Not What You Know, It's How You Know It', *The Journal for Quality and Participation*, July / August 1998, pp.30-33.

17 See Martin Hilbert and Priscila Lopez, 'The World's Technological Capacity to Store, Communicate, and Compute Information', *Science*, Vol.332, No. 6025, 1 April 2011.

government must adhere. All of this will place different demands on the workforce and the ISR Enterprise needs to be investing now in new competencies; improving workforce skills; and better coordinating the workflow of people, resources and materials.

A decade or so ago, intelligence was made up of information from human intelligence, signals intelligence, imagery intelligence, and so on, with only a very small part coming from open source information. Today, that has changed quite significantly, with so much more information being obtained from open sources.

This freely accessible information is one of the driving factors behind today's ISR imperatives. Another factor is the tight international and national fiscal situations that are forcing ISR agencies to evaluate their priorities, including how they collaborate and how they invest in current capabilities versus the next generation of capabilities. Thus, the contemporary ISR capability must be agile and integrated with other agencies and partners, and the ISR community must have a strong understanding of the operational environment, which includes understanding of social issues, social licence and use of social media.

While a clear factor is technology, any focus on technology must not lose sight of the people dimension – of the human in the loop of the intelligence cycle. The role of ISR is to provide the information that leaders need to be able to make better decisions; so, the ISR Enterprise must guard itself against being pushed and pulled by technology alone.

Australia does seem to be on the cusp either of continuing its modest trajectory in improving ISR or of seizing the moment and driving step-change improvements that will demand adopting a whole-of-nation approach, improving public engagement, accelerating the data-to-decision cycle through leveraging the benefits of Big Data, and synchronising ISR capabilities. This *Kokoda Paper* recommends pursuing these step-change improvements through the four new policy approaches identified, as well as continuing to improve Australia's ISR organisations, capabilities, and international and national cooperation.

RECOMMENDATIONS

A number of recommendations flow from the discussion in this Paper. Some modest improvements could flow from a more aggressive pursuit of the current trajectory – in improving existing organisations, capabilities, international relationships, and national cooperation. However, far greater improvement would come through also pursuing four new policy objectives: adopting a whole-of-nation approach, improving public engagement, accelerating the data-to-decision cycle through leveraging the benefits of Big Data, and synchronising ISR capabilities. The major recommendations suggested in this Paper that pertain to each of these objectives are summarised below.

Improving the Current Trajectory

- Mapping the current ISR landscape would help establish a solid foundation for the future positioning of ISR as a national capability, both in terms of making the most out of Australia's current organisations (in removing any duplication) and getting more out of existing capability through greater integration and improved information sharing.
- Australia needs to select a standards framework to facilitate improved integration and collaboration across the ISR Enterprise, as well as with international partners.
- It is time to move away from a systems-engineering perspective for acquisition of ISR capability to a software-engineering approach that is better-suited to short life-cycle and software-dependent ISR capabilities.
- While Australia's agencies have evolved an effective policy-coordinating mechanism at a national level, there remains a lack of synchronisation in funding, capability development and maintenance, and standard setting, which conspire against achieving a true national-level ISR capability, and which needs to be remedied.

Adopting a Whole-of-Nation Approach

- The current sense of cooperation that exists across the ISR Enterprise needs to be captured and evolved into a new culture centred on closer collaboration. Thus, there is a need to create a more strategic design to ensure that enhanced collaboration across agencies can be achieved. In this respect, it is vital to incorporate non-Commonwealth government organisations such as academia, industry and other civic actors in the ISR Enterprise.
- Increased investment is needed to facilitate a move to a whole-of-nation capability that will, as it matures, deliver efficiencies, particularly through rationalisation (and thus removal of duplication) and better integration of processes, people, technology, and administrative arrangements.
- The ISR funding process must become more systematic to remove peaks and troughs that can affect the quality of analysis.
- With the increased focus on the Indo-Pacific, Australia needs to expand its partnering role with the United States in terms of ISR across the region, as well as in space and cyberspace.
- Australia could also do more to develop best practice in the area of ISR infrastructure resilience and transfer this to benefit regional countries that are still in the early stages of developing and connecting their ISR infrastructure.

Improving Public Engagement

- In developing a sovereign ISR capability for protecting national borders and beyond, the Government needs to focus on areas of national interest that do not compromise the rights, privileges and privacy of its citizens.
- The role of the Inspector-General of Intelligence and Security could be used more in improving engagement with the wider community, drawing on the sense of trust that exists with the Australian Defence Force, and including greater collaboration with the Privacy Commissioner.

- Public fears around the invasion of privacy need to be allayed, which demands greater transparency from the Government and public officials. But it is more than transparency as the public can also act as a resource; thus improved public engagement is needed.

Accelerating the Data-to-Decision Cycle

- Leveraging commercial advances in Big Data can improve decision-making; however, there are legal roadblocks and technological and cultural problems to sharing data which need to be overcome. A plan is needed for taking advantage of Big Data to speed up the decision cycle.
- The ISR Enterprise can learn from how successful businesses have used Big Data to improve their competitive advantage through meeting three challenges - identifying the information and how and where it is stored, tagging the data to allow its characteristics to be identified, and running the data through an algorithm that allows it to be collated and presented to an analyst.
- It is quite likely that competence and capability in Big Data will become a mandatory requirement for future operations with the United States – and Australia will need to address this if it wishes to continue to access US ISR capability in future.
- Big Data analytics have a potentially significant role in helping to manage the flood of data and assisting analysts to focus their efforts on analysing content rather than searching for relevant information. Improvements in tools and techniques are needed to support the search and analysis of ISR data.
- Big Data will not solve the challenge of balancing the need to protect information with the potential benefits of sharing. Thus, there is a need to develop a culture, supported by corresponding policies, that incentivises data sharing for the greater good as well as more sophisticated risk-assessment models and techniques around that sharing.
- Social Media Intelligence (SOCMINT) needs to be developed as a coherent academic discipline and distinctive intelligence tradecraft.

- The Australian Government also needs to work in collaboration with data management and social media companies to improve Australia's national privacy principles and to establish guidelines that will strike a balance between privacy rights, security and commercial interests.
- There is a pressing need for the ISR Enterprise to address how the necessary skills will be recruited, developed and retained, which will demand innovative collaborative partnerships with the private sector.
- Australia needs to adopt an 'enterprise architecture' approach that allows, from a technical perspective, the removal of proprietary interests (such as standards and protocols) that affect interoperability, and the removal of obstacles imposed through stove-piped acquisitions.
- A program-centric approach is also needed to improve the approvals process and support faster project cycle times and evolutionary acquisition for short life-cycle and software-dependent ISR capabilities.
- The new fifth-generation capabilities such as the Joint Strike Fighter and Air Warfare Destroyer will bring profound changes to the ISR Enterprise around data management and data security, and Australia needs to start planning for those changes now.

Synchronising Capabilities

- The geospatial data requirements of Defence projects already in the pipeline need to be more satisfactorily addressed. Joint force integration and the need for innovation are vital and demand greater attention prior to First Pass consideration of capital projects.
- There are many ISR projects in train but there needs to be a clear capability manager to ensure these are being phased-in effectively and integrated. In Defence, this would sit best with a Three-Star military officer. For whole-of-government, this should sit with a Band-Three officer in the Department of the Prime Minister and Cabinet. It might also be worth examining the merits of appointing a military Two-Star ISR Commander.

- ISR needs to be viewed as a game-changer in the region; however, any real ISR capability needs to be connected to the US Pacific Command (PACOM) and the US Marines in Darwin. Greater attention needs to be focused on deployed forces and their ISR requirements, particularly with respect to responsibility for deployed systems.
- Defence ISR must improve engagement with the capability managers; adopt a program approach to capability development for ISR; bring industry in as an integral part of the capability development process and ensure industry aspects are considered early, appropriately and consistently; and make better use of the CTD and RPDE programs.
- Australia will need to leverage the lessons learned by the United States in its rapid build-up of its separate, Service-centric DCGS networks and its consequent development of Defense Intelligence Information Enterprise (DI2E), and monitor future developments.
- Australia needs to improve its Processing, Exploitation and Distribution (PED) capability to equip teams of analysts with software tools and give them the ability to share their products with other analysts over the network provided by the ISR Integrated Backbone.

Kokoda Paper No 18, April 2014

Getting it Right: Integrating the Intelligence, Surveillance and Reconnaissance Enterprise

Intelligence, Surveillance, and Reconnaissance (ISR) functions are essential for effective operations spanning military, border protection and law enforcement activities, as well as in strategic decision-making. These functions provide greater situational awareness and better predictive intelligence necessary for superior decision-making at all levels. ISR synchronises and integrates the planning and operation of platforms, sensors, data, and people.

The ISR process must be treated as an integrated process, moving it in complexity, speed, and effectiveness beyond the current model of inter-agency cooperation. Australia can continue its modest trajectory in improving ISR or it can drive step-change improvements that will necessitate adopting a whole-of-nation approach, achieving closer engagement with the public, accelerating the data-to-decision cycle by leveraging the benefits of Big Data, and synchronising ISR capabilities.

Kokoda Foundation

About the Kokoda Foundation

The Kokoda Foundation has been established as an independent, not-for-profit think tank to research, and foster innovative thinking on, Australia's future security challenges. Visit our website at www.kokodafoundation.org

ISSN 1833-1459