WHITE PAPER | 1-2019

THE FUTURE OF THE

NATIONAL INTELLIGENCE ENTERPRISE

IN AUSTRALIA

DECEMBER 2019

PREFACE

The Australian Institute of Professional Intelligence Officers (AIPIO) Inc is committed to growing the intelligence body of knowledge through fostering scholarship, professionalization of practice, support to major intelligence research projects, and professional collaboration amongst practitioners at our events.

Each year, AIPIO promotes a theme to focus our investment in thought leadership. In 2019, the theme was 'An Emerging Intelligence Enterprise' – which aligns with the core proposition in the 2017 Independent Intelligence Review, and the many related initiatives now underway.

The changing nature of 21st century intelligence demands greater connectivity and collaboration. We need to move beyond the traditional concept of intelligence professionals and the intelligence 'community' to realise a strengthened, diverse intelligence 'enterprise' spanning jurisdictions, government agencies, business, finance, technology, and other partners. It is the sharing and integrating of individual capabilities and areas of excellence between these groups that will lead to strong collective performance and outcomes, to effectively leverage change and identify opportunities for collaboration.

Curating and supporting the burgeoning intelligence profession of tomorrow across multiple domains of practice requires strategic management and transformational change. AIPIO activities in 2019 — especially the national conference — explored this emerging landscape in Australia and beyond, especially what it means for capability planning, organisational development, and analytic rigour.

AIPIO has captured the insights generated during this year and given them a forward-looking focus. This White Paper (1-2019) entitled *'The Future of the National Intelligence Enterprise in Australia'* offers four alternate futures highlighting challenges and opportunities for all stakeholders in the intelligence profession over the longer term.

Dr Phil Kowalick, MAIPIO
President, Australian Institute of Professional Intelligence Officers (AIPIO) Inc

CONTENTS

EXECUTIVE SUMMARY

The 2017 Independent Intelligence Review (the 'Intelligence Review') found that because of transforming geopolitical, economic, societal, and technological changes, the national intelligence community will be faced with challenges that will intensify over the coming decade. The Intelligence Review's recommendations broadly cover four priority areas: the co-ordinating structures of the intelligence community, new funding mechanisms to address capability issues, the streamlining of legislative arrangements, and measures to further strengthen the state of trust between the intelligence agencies and the Australian community of which they are part.

This White Paper outlines four alternate futures for the national intelligence enterprise. The futures are exploratory and do not attempt to predict the future of the national intelligence enterprise but rather sketch out plausible dynamics and choices that could give rise to each of them. The four alternate futures do not represent all the futures for the national intelligence enterprise, but they offer a basis for challenging deeply held assumptions, and may assist in generating insights, or at least promoting a dialogue about a change agenda. The emerging future is likely to be messier – perhaps reflecting a combination of elements of the different scenarios outlined below.

- **Scenario 1 – Bureaucratic Enterprise.** The NIE embraced incremental reform but remained weighed down by hierarchy, risk aversion, and the pursuit of efficiency. While intelligence agencies can point to solid processes and comprehensive metrics, there has been little or no performance improvement.
- **Scenario 2 – Fractured Enterprise.** The NIE reform agenda falters along deep cultural lines, fomenting an unhealthy struggle for influence and resources. Intelligence support became uneven as deep expertise became compartmented, and support was directed towards preferred clients.
- **Scenario 3 – Obsolescent Enterprise.** Initially, the NIE refused to acknowledge the need for transformative change, complacently believing their legacy would shield them from a changing world. Eventually the NIE was unable to build the momentum to change fast enough as the wider democratisation of intelligence rendered agencies obsolescent.
- **Scenario 4 – Dynamic Enterprise.** The NIE boldly pursued the 'enterprise model' and assisted by sustained investment has realised many of the benefits described in The Intelligence Review. Purposeful innovation has positioned the NIE as a global leader in the intelligence field, displaying a high level of collective performance and integration.

This White Paper finds that transformational change will require sustained effort to create the environment for the enterprise approach to be successful. Innovation will be a key imperative to evolve the NIE. The White Paper also stresses that wider intelligence reform — whether in Australia or overseas — is fundamentally cultural. Accordingly, the consideration of challenges and opportunities arising from the scenarios, focus on their implications for intelligence management, intelligence practitioners, and the intelligence profession. The White Paper concludes with a discussion of how the Australian Institute of Professional Intelligence officers (AIPIO) could become a trusted partner in support of the evolving NIE.

INTRODUCTION

Background

The 2017 Independent Intelligence Review (the 'Intelligence Review') found that Australia's intelligence agencies are highly capable and held in high regard by their international partner agencies. The Intelligence Review also found that because of transforming geopolitical, economic, societal, and technological changes, the intelligence community will be faced with challenges that will intensify over the coming decade.

To address these challenges, the Intelligence Review made a series of recommendations to provide a pathway to an even higher level of collective performance. These recommendations broadly cover four priority areas: the co-ordinating structures of the intelligence community, new funding mechanisms to address capability issues, the streamlining of legislative arrangements, and measures to further strengthen the state of trust between the intelligence agencies and the Australian community of which they are part.

What is the National Intelligence Enterprise?

"The Intelligence Review identified the desired end state for the NIE was to become a global leader in the intelligence field."

The Intelligence Review does not define the National Intelligence Enterprise (NIE). The lack of a precise definition may cause confusion in the short term but allows the concept to evolve amid complex dependencies between stakeholders and the tempo of intelligence activities at the national level. Key phenomena observed in social systems – competition, specialization, co-operation, exploitation, learning, growth, and several others – are likely to influence the evolution of the NIE. The Intelligence Review identified the desired end state for the NIE was to become a global leader in the intelligence field.

Approach of the White Paper

"The White Paper adopts the scenario method – which is a core concept and one of the most widely used methods in foresight studies."

This White Paper addresses the focal question: 'What is the future of the National Intelligence Enterprise in Australia' with a time horizon of 2030. The White Paper adopts the scenario method – which is a core concept and one of the most widely used methods in foresight studies. This application of the scenario method is exploratory not predictive — positing that the future is neither predictable nor pre-determined but can be affected by individual choices and decisions leading to alternate futures. The scenario method also helps to stimulate creativity and to break from the conventional obsession with present and short-term problems.

Structure of the White Paper

This White Paper considers pertinent drivers of change over the next decade, outlines four scenarios for the future of the NIE, and the dynamics and choices that could give rise to each of them. The paper stresses that intelligence reform – whether in Australia or overseas - is fundamentally cultural. Accordingly, the consideration of challenges and opportunities arising from the scenarios, focus on their implications for intelligence practitioners, intelligence management, and the intelligence profession. The White Paper concludes with a discussion of how the Australian Institute of Professional Intelligence officers (AIPIO) could become a trusted partner in support of the emerging NIE.

DRIVERS OF CHANGE

Drivers of change are likely to create movement in the possibility space and influence the evolution of the NIE over the next decade. These illustrative drivers are neither equally important nor are their outcomes equally uncertain. The drivers may have multiple possible states in the different scenarios.

National Security Outlook

Australia's security environment is becoming more contested and will remain dangerous for the foreseeable future. The unprecedented change occurring in global geopolitical circumstances presents an increased likelihood that in the nearing years, the world could experience a series of massively transformative events — some of which will seemingly come out of the blue. Crowding of the national security agenda will make prioritisation more difficult – and with a tendency to focus on the intelligence problem du jour – could lead to over-concentration on a single threat.

Conflict in East Asia. The prospect of prolonged strategic competition between the US and China, and the potential for that competition to slide into military conflict, should directly shape Australian national security outlook over the coming decade.

Conflict in North East Asia. Tension on the Korean Peninsula will likely rise in the near term because of the collapse of diplomacy between the US and North Korea towards the goal of denuclearisation of North Korea. Renewed provocations from the North would pressure the Trump administration to reassert a new maximum pressure campaign without good prospects for a return to diplomacy.

Conflict in the Middle East. Tensions between the US and its partners in the Middle East arrayed against Iran continue to grow, and military conflict in the near term, perhaps stemming out of another military incident similar to the Iranian shooting down of a USAF Global Hawk UAV, or a direct Iranian attack on a US ally in the region, can't be dismissed.

Intelligence Reform Agenda

Improving coordination is a prevailing orthodoxy of intelligence reform in Australia. Intelligence reviews – both within Australia and overseas – have repeatedly identified information sharing, interoperability and strong coordination among agencies are critical elements of an effective intelligence response to complex, transnational security challenges. The Intelligence Review also called for the strengthening of these elements in the contemporary intelligence reform agenda. Yet the intelligence reform agenda is not underpinned by a national intelligence strategy or long-term vision of the role intelligence will play in furthering Australia's national interests.

Importantly, the Intelligence Review did not arise because of an existential threat to Australia and lacked the gravitas to shift the perception of national security and propel the Australian response. Historically, decisive action took place only after a disaster had occurred or specific weaknesses had been laid bare. Both the United States and the United Kingdom took bold steps after the attacks of 11 September 2001 and 7 July 2005 respectively to strengthen the co-ordination and integration of their intelligence communities. In Australia, between 2002 and 2010, successive federal governments promulgated 45 new security laws.

Indeed, the 'enterprise model' may not prove to be the panacea for reform. First, the volume of information is so vast that even with the continued rapid advances in data processing it cannot be collected, stored, retrieved, and analysed in a single database or even network of linked databases. However, this proposition may be challenged by growing investments in artificial intelligence and quantum computing. Second, legitimate security concerns limit the degree to which classified information can safely be shared, especially as more porous organisational boundaries increase the potential damage done by insider threats. And third, the different intelligence services and the subunits of each service tend, because information is power, to hoard it. Intelligence reform will remain fundamentally cultural.

> *"Crowding of the national security agenda will make prioritisation more difficult ..."*

> *"... the intelligence reform agenda is not underpinned by a national intelligence strategy or long-term vision of the role intelligence will play in furthering Australia's national interests."*

Public Sector Reform

The NIE is bureaucratic in character, comprising institutions and agencies often insulated by different cultural practices. The 2019 Independent Review of the Australian Public Service (the 'APS Review') echoed many of the enterprise design imperatives in the Intelligence Review, viz.:

> 'In a complex, changing world, the APS needs to work flexibly and nimbly across organisational boundaries. It needs to respond dynamically to change, and to harness the right APS expertise, perspectives, and resources to deliver seamless services and solve problems. It needs to empower people and teams to deliver outcomes, not deal with process and hierarchy. And in an era of continued fiscal pressure, the APS needs carefully prioritised investment in capital, including digital transformation, and needs to provide robust, evidence-based advice to inform government budget decisions.'

"This wave of public sector reform is likely to buoy the intelligence reform agenda."

Reforming the APS to achieve this change is ambitious. Partly this is because the APS itself is big and diverse, consisting of more than 190 separate entities and companies, hundreds of boards and committees, and many subsidiaries and other arrangements, all with an annual budget around $430 billion. But transformational change will be necessary to deliver an APS that is fit-for-purpose to meet the rising expectations of Australians and emerging opportunities and challenges – economic, social, technological, and geopolitical over the next decade and beyond. This wave of public sector reform is likely to buoy the intelligence reform agenda.

Intelligence Workforce

Technological enablement is a dominant feature of the intelligence reform agenda but integrating digital technologies that allow collaboration without adopting complementary social practices will diminish the benefits afforded by the new technologies. Notwithstanding technological enablement, intelligence will remain a 'people business' but the character of the workplace and management imperatives would change in response to the unprecedented presence of four 'generations' in the workplace, namely Baby Boomers, plus Generations X, Y and Z.

"... intelligence will remain a 'people business' but the character of the workplace and management imperatives would change ..."

Over the next decade, Generation X will dominate management levels of the intelligence community, with Generation Y providing the bulk of active practitioners. By 2030, the leading edge of millennials will be nearing 50, and they and Gen Z will make up most of the workforce. Two key challenges are the leaching of corporate knowledge in the wake of Baby Boomer decline, and the lack of innate, institutional loyalty by Generation Y.

More broadly, the intelligence workforce is likely to become a national asset, and more important in whole-of-nation security planning, as both foreign nation states and non-state actors resort to hybrid or grey-zone conflict. Increasing the diversity of the intelligence workforce beyond comprising multiple generations, to include varying cultural heritage, worldview, and career aspiration will evolve a 'different' national asset better able to comprehend and navigate the post-normal world.

Wild Cards

Wildcards are low-probability, high-impact events that happen very quickly, with potentially significant consequences for the focal question – the future of the NIE. For example, the COVID-19 pandemic, which began as a public health issue with deepening economic impacts could pose enduring national security concerns. Consideration of wild cards in the context of the scenarios helps surface new uncertainties and different approaches for future action that may not emerge from the more logical structure of a scenario framework.

Weakening of International Intelligence Cooperation. Five Eyes is one of the world's most successful intelligence gathering and sharing partnerships – at the core of Australia's national security strategy — now under new stress over Chinese participation in 5G telecommunications networks. The Fives Eyes partners are not (not yet, at least) unified on this 5G issue, with New Zealand, Canada and Britain having more nuanced and perhaps questionable positions. Huawei represents a significant challenge to the future of Five Eyes, which could lead to the weakening of international intelligence cooperation. Also, the intelligence-sharing deal between South Korea and Japan is a linchpin of trilateral security cooperation but is complicated by painful, wartime history.

Prioritisation of Domestic Threats in the National Security Outlook. The management of threat could become more challenging with the emergence of new internal and intangible threats bearing upon national security and competing for scarce government resources. This growing threat complexity may dislocate an intelligence and security apparatus focused on the external environment and constrained by policy inertia. Under these circumstances, and in the absence of reliable means for measuring NIE effectiveness, political interest in external threats might weaken and constrain the intelligence reform agenda.

“ Consideration of wild cards in the context of the scenarios helps surface new uncertainties and different approaches for future action ... ”

ALTERNATE FUTURES

This White Paper outlines four scenarios for the future of the national intelligence enterprise, the dynamics and choices that could give rise to each of them, and their implications for intelligence managers, intelligence practitioners, and the intelligence profession. The four scenarios are exploratory and do not attempt to predict the future of the NIE but rather sketch out conceivable alternative futures and some of the implications for key stakeholders. The four scenarios do not represent the totality of NIE futures, but they offer a basis for challenging deeply held assumptions, and may assist in generating insights, or at least promoting a dialogue about a change agenda. The actual course of events is likely to be less contained – perhaps reflecting a combination of key elements of the different scenarios outlined in this White Paper.

Scenario One – Bureaucratic Enterprise

The Bureaucratic Enterprise has hastened slowly to embrace the intelligence reform agenda. Unable to break from the conventional obsession with present and short-term problems, the Bureaucratic Enterprise placed a strong emphasis on business planning rather than strategy. The Bureaucratic Enterprise is process and compliance driven offering little or no performance improvement. Limited performance improvement has been disguised by ambiguous performance metrics for the national security community – both at the intelligence agency level, and for the enterprise.

“... process and compliance driven offering little or no performance improvement.”

Still present in the Bureaucratic Enterprise architecture are the traditional hard functional and organisational boundaries – favoured for their contribution to efficiency. Efficiency is still considered a pre-eminent goal, but notions of simplifying tasks and centralising authority limits the Bureaucratic Enterprise from responding effectively to the rapidly changing environment created by technology. Efficiency fails to make room for adaptability in structures, processes, and mindsets.

Much of the Bureaucratic Enterprise capital budget has been consumed by addressing accumulated technical debt in legacy ICT systems deemed necessary to ‘keep the lights on’ within individual agencies but constraining enterprise solutions for improved collaboration, coordination, and digital transformation. Expanded scrutiny by the Parliamentary Joint Committee on Intelligence and Security (PJCIS) into capital expenditure increases competitive tension between agencies, which constrains inter-agency collaboration.

However, the Bureaucratic Enterprise did deliver some early demonstrable agency-level gains from incremental change but a poor shared understanding by agencies of the ‘intelligence enterprise’ concept have limited the impact of gains at the enterprise level. Despite a series of leaders’ best intentions, the Bureaucratic Enterprise remains bloated and dominated by a self-reinforcing culture that unintentionally rewards intelligence managers who suffocate more transformative innovative ideas that might threaten the established way of doing things.

“... plagued by ongoing barriers to improved coordination and collaboration ...”

The Bureaucratic Enterprise has also been plagued by ongoing barriers to improved coordination and collaboration, including security classification systems, poor ICT connectivity, and embedded cultural practices. The trialling of alternative options for Top Secret (PV) clearances – intended to alleviate Australian Government Security Vetting Agency (AGSVA) backlog — proved ineffective, and unsupported by Australia’s Five Eyes partners. Consequently, there has been token engagement of external expertise, and greater emphasis placed on APS-wide generalist skills than building specialist expertise in areas such as analytic methods.

Indeed, the more prominent place of intelligence in modern society has reinforced risk-averse behaviour especially where assessments can produce unintended effects on Australians. The dynamic threat environment, actionability, and risk has distorted the balance of production between current and estimative intelligence, emphasizing the former, and resulting in the loss of a strategic perspective across the Bureaucratic Enterprise.

Scenario Two – Fractured Enterprise

In past intelligence reforms, founded on existential threats such as 9/11, individual agencies in the enterprise grew simultaneously, avoiding hard questions about where funding should be prioritised. In the Fractured Enterprise, pursuing the intelligence reform agenda has sharpened distinctions between the resourcing, power, and influence of individual agencies and institutions in the enterprise. Individual agencies and institutions in the Fractured Enterprise were uncomfortable ceding control by thinking and acting outside of traditional boundaries – a mindset shift that was essential for an enterprise model to be successful.

The emergence of new and unfamiliar domestic threats required capabilities outside the Fractured Enterprise. The widespread use of the private sector to augment the enterprise led to a hollowing out of expertise in the public sector. Key areas of expertise were concentrated in individual agencies and institutions because contractual arrangements focused too heavily on competition and not enough on collaboration across the enterprise. Advancing the interests of individual agencies was given more weight in decision making rather than taking advantage of the intellectual capacity and administrative experience the enterprise had to offer.

"... sharpened distinctions between the resourcing, power, and influence of individual agencies and institutions in the enterprise."

Despite new challenges, funding for strategic responses to technological change favoured specific agencies closer to issues at the core national security agenda. Individual agency heads sought to please key political clients in other ways, to demonstrate responsiveness by devoting resources to more tactical and immediate support than to strategic and longer-term advice, and intelligence activities with dubious domestic and international benefits. The 'intelligence enterprise' concept grew increasingly ambiguous and irrelevant.

Minimising political risk became a key concern for the Director of National Intelligence (DNI), but without the authority to direct resources across and between agencies the DNI lacked the clout to mitigate political risk. However, whistle-blower concerns about politicisation triggered expanded uncomfortable public scrutiny by the Inspector-General of Intelligence and Security (IGIS). Alignment with partisan concerns undermined the confidence of the Parliament and the public in the Fractured Enterprise as an apolitical institution.

"... the intelligence workforce became careerist – pursuing personal advancement without regard to the enterprise ethos and mission."

In the Fractured Enterprise, the intelligence workforce became careerist – pursuing personal advancement without regard to the enterprise ethos and mission. Professional development became a means to outshine others rather than to improve the quality of intelligence collaboration, production, and service. Intelligence managers and practitioners kept a keen eye on the political agenda of their own agencies and institutions, regarding the professionalisation of intelligence practice as an abstraction and distraction from ruthless execution of assigned tasks.

Scenario Three – Obsolescent Enterprise

The Obsolescent Enterprise has been too slow to recognise and adapt to disruption arising from the external democratisation of intelligence, and growing contestability of intelligence assessment. There is now much more scope for constructive competition of ideas and many sources of expert advice on intelligence issues, but the Obsolescent Enterprise is more inward-looking and seemingly anonymous as it does a poor job recording, documenting, analysing, or distilling lessons from its own past experiences.

"... subscribed to the proposition that the work of tomorrow will be the same as the work of today."

The Obsolescent Enterprise subscribed to the proposition that the work of tomorrow will be the same as the work of today. Decisions are top-down, and the intelligence workforce interactions are transactional and unlikely to lead to new opportunities or innovations. Within agencies, innovation is incremental using familiar approaches to help improve the existing system. Beyond agency boundaries, collaboration and coordination efforts become code for control, ensuring everyone 'sings from the same song sheet', promoting 'groupthink' and constraining transformation.

Intelligence managers, who have reached their position in the Obsolescent Enterprise by learning the intricacies of the current 'system,' openly or subversively resist efforts to change the system. The trajectory to this future is managerial in nature, as it represents a system in use, and managers who must keep it running, it is the way that things get done today. No one has great expectations of quality or public acceptance. Nothing is ventured, nothing is threatened. The level of intelligence support has remained desultory for so long that the Obsolescent Enterprise has settled into a comfortable rut.

The lack of interest and investment in professionalising intelligence practice across the Obsolescent Enterprise has led to great variation in the competence and skill of individual analysts, uncertainty regarding the very duties of intelligence practitioners and an overall diminution in the role that intelligence analysis could play in decision making. A doctrinaire embrace of the familiar 'intelligence cycle' production model has led to practices – and intelligence architectures — better suited to traditional 'complicated' settings rather than the prevalent complex settings confronted by the enterprise as the world moved from a 'data-poor world with relatively predictable settings' to a 'data-rich world with unpredictable settings.' The failure to hold intelligence practitioners accountable to formal professional standards prevents their services from being fully utilized. In the Obsolescent Enterprise, intelligence consumers have no assurance that intelligence analysis is consistently reliable.

"... intelligence practitioners concerned about the future of the enterprise, have chosen to leave for other opportunities, and others have become fearful and less engaged."

For the Obsolescent Enterprise, sustaining the level of funding for the enterprise has proven difficult in the absence of a major national security incident. Mounting legacy technical debt constrains investment for transformation and technical barriers to enterprise-wide collaboration prove intractable. The loss of political interest in intelligence transformation coupled with the Government's insistence that performance targets must be commensurate with the resources the Government makes available has constrained funding to keeping the lights on.

In the Obsolescent Enterprise, the long period of heightened uncertainty about the viability of the enterprise has taken a toll on workplace culture. Many of the best intelligence practitioners concerned about the future of the enterprise, have chosen to leave for other opportunities, and others have become fearful and less engaged. The wider lack of operational agility precludes the agencies and institutions of the enterprise from making the quick pivots necessary for surviving and thriving.

Scenario Four – Dynamic Enterprise

The Dynamic Enterprise moved boldly and decisively to implement the reform agenda outlined in the Intelligence Review. The impact of the intelligence reform agenda was not immediate or overly disruptive, but over time was transformational. The Dynamic Enterprise consciously leaned into changes and counterintuitive activities at the precise moments when it is most uncomfortable to do so, especially when the forces of inertia and gravity was pushing it toward a predictable outcome.

The Dynamic Enterprise stresses the importance of intelligence architecture over intelligence process, highlighting the limitations of traditional intelligence models in navigating a complex problem space. The Dynamic Enterprise has taken full advantage of new technologies to facilitate collaboration, allow more responsive service delivery to clients, as well as driving increased efficiency. Networks have become the main institutional design feature of the Dynamic Enterprise, allowing innovation to emerge from anywhere and ripple across the enterprise at the speed of relevance.

"... recognised that efficiency is necessary but no longer sufficient to be successful."

Absent from the Dynamic Enterprise are the traditional hard functional and organisational boundaries – favoured for their contribution to efficiency – because it is recognised that efficiency is necessary but no longer sufficient to be successful. For the millennials in the intelligence workforce, workplaces are now seen more as networks than as hierarchies. Intelligence practitioners are more likely to seek out the people they need to work with, at any level, to get their work done. Intelligence managers who are frustrated by anyone who does not work through proper channels are seen by millennials as a bad user experience. The best intelligence practitioners do not need to be managed - they need guidance, because they're already self-motivated and brimming with ideas.

Capability development across the Dynamic Enterprise becomes easier as its agencies and institutions stopped thinking in terms of 'owning' capability but rather considered that they are 'leasing' and 'leveraging' capability in a whole of nation context. Technological innovation and the rise of open source intelligence (OSINT) weakened the basis for longstanding information security protocols, especially as OSINT displaces traditional sources. These evident gains from joint capability development and systems integration on an enterprise-wide basis offered up a 'collaboration' dividend.

The Dynamic Enterprise has defined the knowledge, skills and abilities needed for each specialty related to intelligence production, providing more nuanced understanding of the education, training and professional development needed for each specialty. Over time, this investment in the intelligence workforce has led to greater consistency and reliability in intelligence production, and improvements in both individual and organisational performance.

"... stopped thinking in terms of 'owning' capability but rather considered that they are 'leasing' and 'leveraging' capability in a whole of nation context."

CHALLENGES AND OPPORTUNITIES

"The key recommendations of the Intelligence Review (are) probably insufficient to stimulate further information sharing, collaboration, and integration – which are all cultural in nature."

"Exaggeration of the challenges to reform is more often a managerial failure rather than an organisational one."

The four scenarios are differentiated based on how empathically the agencies and institutions in the NIE embraced the intelligence reform agenda outlined in the Intelligence Review. The scenarios highlighted that enterprise planning privileging efficiency will deprive organisational decision makers of a full range of alternatives. The key recommendations of the Intelligence Review — creation of the Office of National Intelligence (ONI), legislative reform, joint intelligence capability development, and strategic human resource management of the intelligence workforce are timely and appropriate but, by themselves, probably insufficient to stimulate further information sharing, collaboration, and integration – which are all cultural in nature.

For reform to be successful, the intelligence workforce needs to come along and ensure that change is deeply embedded in structures and systems. Otherwise, good ideas will inevitably be lost through poor implementation. The scenarios highlighted that many elements of capability – organisations, people, systems, and tradecraft — will need to change concurrently and yet remain synchronized. Capability development will become easier if organisations stop thinking in terms of 'owning' capability but rather consider that they are 'leasing' and 'leveraging' capability. The arrangements needed to effect coherent capability development will operate quite independently of individual organisational structures. The NIE will need to become less organisation-centric and more interdependent as pressure grows from self-organisation through the proliferation of collaboration channels. A longer-term perspective on strategic change is also needed to aid futureproofing of intelligence capability, especially through partnerships extending beyond the traditional intelligence community.

The key recommendations of the Intelligence Review should be only the beginning of a larger necessary reform. The likely novelty of future threats requires commensurate novelty by the NIE. But it is challenging to take effective action to mitigate the risk of something that hasn't occurred previously. The scenarios highlighted that a key challenge will be making the NIE more receptive to innovation in multiple dimensions — conceptual, organisational, process, and technological. In its most basic form, innovation is simply the act of introducing something new; however, if innovation is to have any real value for the NIE, it must have a purpose — introducing something new to achieve a specific change — and it must achieve its purpose to be successful.

Intelligence Managers

The Intelligence Review judged that the NIE 'would benefit from greater investment in the development of its current and future leaders.' Exaggeration of the challenges to reform is more often a managerial failure rather than an organisational one. The scenarios highlighted that issues beyond the characteristics of individual intelligence products or services, will determine the success of intelligence effort. The agencies and institutions within the NIE will require an intelligence effort more closely attuned to collective objectives. Organisational and functional barriers should be removed to allow the collective knowledge, skills, and behaviours of the entire NIE to be mustered into something that is greater than the mere sum of its parts. The intelligence management function will be core to achieving this synergistic effect.

Digital technologies will become more pervasive and integrative, making the agencies and institutions in the NIE more pliable and porous, and the intelligence workforce more questioning, assertive, and independent. The management imperatives of this 'new organisation' are to continually improve as part of its normal functioning; to be intelligent, critical, and open; and to be creative and capable of eternally transforming themselves while sustaining a sense of purpose and direction. Intelligence managers will need to ask, 'As technology frees us to do different work, what are the mindsets, tools, and capabilities we need in order to embrace the value that humans can bring to work, and what types of investment does the enterprise need to make to support that?' These investments should seek to create a work environment — which includes the physical and virtual spaces as well as the management systems and practices — that encourages (and requires) intelligence practitioners to use their human capabilities to find new sources of value for the NIE.

Reform objectives will be achieved by people. Traditionally, many management roles have involved defining individual tasks and even specific processes for completing them. Tomorrow, tasks that can be prescribed will be more often automated, ensuring that fewer employees perform repetitive tasks, and more are engaged in personalizing services, innovating offerings, and creatively solving problems. In the NIE, intelligence managers must set the conditions for a culture of innovation; a culture eager to adopt new ideas, and a culture committed to learning and improvement. Without an innovation culture, initiatives to create change and incorporate change will have no place to take root and grow.

Intelligence Practitioners

As the 9/11 Commission concluded, there is a risk that the practices used to succeed in the past will not serve intelligence so well into the future. The success of intelligence at any time depends on anticipation and adaptation to the opportunities and challenges posed by emerging conditions, technical possibilities, and information flows. Evolution of the NIE requires that innovation and problem solving become the products of teamwork, not a single architect. Yet, for example, intelligence practitioners currently do not experience high levels of individual autonomy due to involvement of management in approving the dissemination of most finished intelligence analysis.

“... innovation and problem solving become the products of teamwork, not a single architect.”

The future will punish intelligence practitioners committed to employing old methods to solve new problems. Old methods and mindsets need to incorporate knowledge from new domains, such as decision science, network theory and drama theory, if they are to better deal with emerging challenges and opportunities. For example, the pervasive employment of digital technologies and increased automation are changing how people work and what they can contribute to organisational success. Intelligence practitioners should use, develop, and adapt their new skills, tools, and techniques, and develop the capabilities to keep learning and adapting as conditions change.

The changing intelligence workforce – influenced by generational change — will likely relate to cross-community challenges rather than organisational loyalty, so accredited training will be necessary to ensure transportability of qualifications across the intelligence community. Systems standardization across the NIE is unrealistic; however, interoperability and complementarity are worthwhile and achievable design objectives. Innovation in tradecraft through partnerships beyond the NIE offers the only real sustainable competitive advantage in a dynamic threat environment.

“... accredited training will be necessary to ensure transportability of qualifications across the intelligence community.”

Intelligence Profession

Intelligence is a discipline that has not yet been widely accepted as a profession, perhaps due to its relatively small personnel base and lack of external scrutiny. Unlike other recognised professions, intelligence as practiced is unregulated, unstandardized, and lacking in key aspects of a profession. The failure to professionalise has led to great variation in the competence and skill of individual intelligence officers, uncertainty regarding the duties of intelligence officers, and an overall diminution in the role that intelligence could play in decision making. The APS Review calls for deploying a wider range of specialist talent and further investment in the skills, capability, and expertise of the APS workforce. Recognition of intelligence as a distinct discipline requiring a specialist workforce would accelerate the move towards intelligence as a profession.

“... great variation in the competence and skill of individual intelligence officers ...”

AIPIO as a Trusted Partner of the NIE

Professional practice is not immune from change, but the intelligence profession often struggles to give up the tried, tested, and familiar without stimulus. From its beginning in 1991, AIPIO has been committed to the professionalisation of intelligence across multiple domains of practice with the aspirational goal of establishing intelligence as a recognised profession in Australia. AIPIO also has advocated for keeping the practitioner central in intelligence practice. The central role of intelligence managers, intelligence practitioners, and the intelligence profession in intelligence reform makes AIPIO a natural partner in the evolution of the NIE in Australia.

“AIPIO envisages a partnership approach based on an ecosystem model.”

“AIPIO could make key contributions to improve intelligence performance.”

In Australia’s increasingly complex operational environment, the agencies and institutions of the NIE will not be able to go it alone. The Intelligence Review judged that the NIE ‘generally would benefit significantly if external engagement was more systematic and better co-ordinated.’ However, the proposed external engagement was narrowly defined in terms of ‘appropriate and productive exchanges on science and technology issues with publicly funded research agencies, academia and industry within Australia.’ This approach seems anchored to the agencies in the national security community, overly transactional, biased towards the technological dimension of innovation, and unlikely to achieve the desired end state of the Intelligence Review: making the NIE a global leader in the intelligence field.

Alternatively, AIPIO envisages a partnership approach based on an ecosystem model. The ecosystem would comprise a network of cross-industry players who work together to define, build, and execute innovative solutions across multiple dimensions - conceptual, organisational, process, and technological. The ecosystem would be defined by the depth and breadth of potential collaboration among a set of players, with each delivering a component of the solution, or contribute a necessary capability. The power of an ecosystem model is that no single player needs to own or operate all components of the solution, and that the value the ecosystem generates is larger than the combined value each of the players could contribute individually.

Within the proposed ecosystem model, AIPIO could make key contributions to improve intelligence performance:

- Maintain a strategic focus on professionalisation of intelligence practice.
- Focus thought leadership on intelligence management – which is a poorly defined competency – and on analytic methods more appropriate to modern complex operating environments.
- Develop an authoritative formal knowledge base – an Intelligence Body of Knowledge (IBOK).
- Provide a virtual learning facility for the NIE, to support a systematic approach to professional development informed by good practice across multiple domains of intelligence practice.
- Manage an NIE certification program for intelligence managers and practitioners, including the capture of continuing professional development.
- Manage an open innovation network of skilled practitioners with a deep understanding of intelligence practice and able to operate across the innovation value chain.

REFERENCES

Agrell, W. (2002) "When Everything is Intelligence, Nothing is Intelligence." The Sherman Kent Center for Intelligence Analysis. Occasional Papers (1)4 (October) http://www.cia.gov/cia/publications/Kent_Papers/pdf/OPNo 4.pdf

Bates, R.W. (1982). The Intelligence Profession. *American Intelligence Journal*, (4)3, pp.19-23.

Best, R.A. (1996). *Proposals for Intelligence Reorganization 1949-1996.* Congressional Research Service: Washington, DC.

Hackman, J.R. (2011). *Collaborative Intelligence: Using teams to solve hard problems.* Berrett-Koehler Publishers: San Francisco.

Jones, D.M. (2018). Intelligence and the management of national security: the post 9/11 evolution of an Australian National Security Community. *Intelligence and National Security.* (33)1, pp.1-20.

L'Estrange, M., Merchant, S. and Lobban, I. (2017). *Independent Intelligence Review.* Department of the Prime Minister and Cabinet: Canberra.

Lowenthal, M.M. (2018). *The Future of Intelligence.* Polity Press: Cambridge.

McChrystal, S. (et.al.) (2015). *Team of Teams: New rules of engagement for a complex world.* Portfolio Penguin: St Ives.

Peppler, C.B. (2006). *The Future of Intelligence.* Australian Homeland security Research Centre: Canberra.

Pillar, P.R. (2011). *Intelligence and U.S. Foreign Policy: Iraq, 9/11, and misguided reform.* Columbia University Press: New York.

Thodey, D. (et.al.) (2019). *Our Public Service Our Future.* Independent Review of the Australian Public Service. Department of the Prime Minister and Cabinet: Canberra.

Ungerer, C. (2010). Australia's National Security Institutions: reform and renewal, Special Report 34. Australian Strategic Policy Institute: Canberra.

LIST OF ACRONYMS AND TERMS

AGSVA	Australian Government Security Vetting Agency
AIC	Australian Intelligence Community
AIPIO	Australian Institute of Professional Intelligence Officers Inc
APS	Australian Public Service
ASPI	Australian Strategic Policy Institute
DNI	Director of National Intelligence
HUMINT	Human Intelligence
IBOK	Intelligence Body of Knowledge
ICT	Information and Communications Technology
IGIS	Inspector-General of Intelligence and Security
IIR	Independent Intelligence Review (2017)
NIC	National Intelligence Community
NIE	National Intelligence Enterprise
NSC	National Security Community
ONI	Office of National Intelligence
OSINT	Open Source Intelligence
PJCIS	Parliamentary Joint Committee on Intelligence and Security
Scenario	A description of how the future may unfold according to an explicit, coherent, and internally consistent set of assumptions about key relationships and driving forces. The term 'scenario' was introduced by Herman Kahn in the 1950s in connection with military and strategic studies conducted by the Rand Corporation. Kahn used the term for issues related to US public policy, international development, and defence.
USIC	United States Intelligence Community
Wildcard	An early indication of a potentially important new event or emerging phenomenon that could become an merging pattern, a major driver, or the source of a new trend.

About AIPIO

Established in 1991, AIPIO is the peak representative body for the intelligence profession in Australia. Through leadership, advocacy, and innovation, AIPIO will advance the professionalisation of intelligence practice across all domains, ensuring the Institute remains relevant and attuned to the evolving nature of the intelligence professions, the needs of its members, and key stakeholders.

Author

Brett Peppler is the Managing Director of Intelligent Futures Pty Ltd, a management consulting practice providing intelligence-led approaches for managing uncertainty in strategic planning. Brett specialises in the creative application of strategic foresight to help clients frame and navigate complex strategic challenges. Brett has over 40 years of professional experience as an intelligence officer, and is a Fellow, Past President, and Life Member of AIPIO.

Acknowledgements

The author acknowledges contributions from John Schmidt, Travis Cunningham, Taylor Devlin, Riley Allen, and Kaitlyn Frazer.

Disclaimer

The Australian Institute of Professional Intelligence Officers (AIPIO) Inc does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select those vendors with favourable reviews or other designation. AIPIO research publications consist of the opinions of the authors and should not be construed as statements of fact. AIPIO disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

Australian Institute of Professional Intelligence Officers (AIPIO)

Membership@aipio.asn.au | 1300 411 036

Web: aipio.asn.au