



## The Future of Intelligence

by Brett Pepler

This *National Security Practice Note* aims to assess the likely developments in the intelligence profession over the next ten years to 2016.

It presents a synthesis of the viewpoints presented at *Intelligence 2006* conference, run by the Australian Institute of Professional Intelligence Officers (AIPIO) on 17-19 October 2006.<sup>1</sup> *Intelligence 2006* provided an opportunity to muster a range of views from practitioners and other interested stakeholders about where intelligence practice was heading in the short to medium term.

This Note adopts a futures-studies approach to the synthesis, which posits that the future is neither predictable nor pre-determined; however, the future can be affected by individual choices and decisions. In this context, the future-focused views expressed at *Intelligence 2006* are clustered into five themes, which provide the basis for creating four alternate futures. The alternate futures will be used to challenge current assumptions about intelligence. The views expressed in this paper are the sole responsibility of the author and should not be attributed to the speakers or other participants at *Intelligence 2006*.

### Future Themes

The speakers at *Intelligence 2006* offered up numerous insights about the future of intelligence, which for the purposes of this paper are clustered into five themes:

- Threat complexity;
- Human resources;
- Organisational change;
- Systems development; and
- Tradecraft.

### Threat Complexity

*Intelligence 2006* participants generally agreed that the threat environment was becoming more complex, both in terms of the number of near-term, tangible threats and mid-to-long term, less tangible threats likely to emerge from the conjunction of many negative driving forces in the natural environment. The management of threat would become more challenging with the co-existence of tangible and intangible threats bearing upon national security, and competing for scarce government resources. Also, growing threat complexity may hamper an intelligence and security apparatus focused on the current environment, and burdened with policy inertia and tactical drag.

### Human Capital

The issue of generational change in the intelligence profession arose frequently at *Intelligence 2006*. 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. Over the next ten years, Generation X will dominate management levels of the intelligence community, with Generation Y providing the bulk of active practitioners. Two key problems are the leaching of corporate knowledge in the wake of Baby

#### About the author

Brett Pepler is the Managing Director of Intelligent Futures Pty Ltd, an independent consultancy based in Canberra providing intelligence support services. Brett has worked for over 28 years in the intelligence field including extensive experience overseas, and across multiple intelligence disciplines. He has held a number of AIPIO Board appointments, and is currently co-opted to the Board as the Public Affairs Officer (PAO).

Boomer decline, and the lack of innate, institutional loyalty by Generation Y.

### Organisational Change

The dynamism of the operational environment will necessitate adaptive organisations driven by 'sense and respond'<sup>2</sup> mechanisms able to overcome the institutional inertia inculcated through a long engagement with slow-moving, symmetric threats. A recent trend associated with the move towards 'sense and respond' mechanisms has been the growth of intelligence agency staff numbers, resulting in little shared understanding of the role of intelligence, and incoherent guidance for community-wide intelligence capability development. New organisational forms are likely to emerge with core functions being outsourced to the private sector and higher education

sector to dynamically link threat complexity and virtual institutional knowledge. Softer organisational structures may also emerge that would allow intelligence analysts to self-organise; for example, using 'wikis' as the basis of collaboration.<sup>3</sup>

### Systems Development

Participants at Intelligence 2006 bemoaned the lack of systems connectivity, and the resultant constraints imposed on information flows and wider collaboration. Dynamism will demand explicit future-proofing of systems, most likely only achieved at a premium, with transitions from 'dumb' legacy systems exacerbating cost considerations. Technological innovation and the inexorable urge for information to flow freely, which has fuelled the open source information (OSI) phenomenon,<sup>4</sup> will weaken the basis for long-standing information security protocols, especially as OSI displaces traditional sources. Greater local exploitation of national intelligence capabilities is likely to emerge as systems development on a community-wide basis offers up a 'collaboration' dividend. While not replacing human capability, computer-assisted analysis will become the core technology of systems development in the wider intelligence community.

### Tradecraft

Conference participants saw a growth in new theories of practice and types of analysis, especially in the face of pressing demands for actionable intelligence against pervasive but intangible targets. The future will punish analysts 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 actors in the new threat environment. Yet the more prominent place of intelligence in modern society could foster risk-averse behaviour especially where assessments are capable of producing deleterious unintended effects on Australians at home. The dynamic threat environment, actionability, and risk may distort the balance of production between current and estimative intelligence, emphasizing the former, and resulting in the loss of a strategic perspective.

### Alternate Futures for Intelligence

Alternate futures are multiple plausible views of the future usually constructed as word pictures or scenarios, describing the external environment into



The Australian Homeland Security Research Centre undertakes independent, evidence-based analysis of domestic security issues.

*National Security Practice Notes* is a publication series that covers topical issues which are of critical importance to building national and domestic security capability.

*National Security Practice Notes* is part of the research program of the Australian Homeland Security Research Centre.

The Centre's 2006 research priorities include:

- Performance measures for domestic security policy
- The appropriate sharing of security costs and benefits between business and society
- National security capability development
- The role of the private sector security in national security

#### About the author

Athol Yates is the Director of the Australian Homeland Security Research Centre which is a non-partisan think-tank on domestic security.

Athol Yates  
Australian Homeland Security Research Centre  
Tel 02 6161 5143, Fax 02 6161 5144  
PO Box 295, Curtin ACT 2605  
Australian Institute of International Affairs Building  
Level 2, 32 Thesiger Court, Deakin ACT 2600  
info@homelandsecurity.org.au  
www.homelandsecurity.org.au

Copyright 2006. All rights reserved.  
ISSN1449-9630 (Print)  
ISSN 1449-9649 (Electronic)

which an organisation is moving, and differentiated on the basis of one or more highly uncertain variables. Alternate futures allow us to explore and challenge our assumptions about plausible future developments. In this case, the themes derived from *Intelligence 2006* – threat complexity, human resources, organisational change, systems development, and tradecraft - have been woven to create three provocative scenarios; transformation, adaptation, and status quo. The scenarios are structured to align with the key questions (as amended) posed during *Intelligence 2006*:

- Where will Intelligence be in 2016?
- How are we going to get there?
- Who will be involved?
- What have we learnt from the past?

The three scenarios – *transformation*, *adaptation* and *status quo* – do not represent all the future scenarios of intelligence. 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.

### Scenario One – Transformation

In 2016, the intelligence community and the wider body of intelligence practitioners have addressed an increasingly complex threat environment through a renaissance of practice, which has transformed people, processes, organisations and systems. Old models and methods have lost their potency, prompting a structured and sustained search for new knowledge.

*Transformation* was possible through an urgent and pervasive understanding of the need for change. People have been central to the transformation; valued for their individual contributions, and considered useful wherever they seek to make their contribution in the wider intelligence community. Intelligence organisations do not measure capability in terms of their staff numbers but rather in their ability to build relationships across the community to muster talent where and when it is needed for the common good.

Capability shortfalls in the intelligence community are being overcome by robust partnerships with the private sector. Future proofing of intelligence capability is achieved through contractual arrangements and service level agreements. Internal leverage is achieved by the proliferation of avenues

for tactical elements to exploit national capabilities, the self-organisation of analysts across the community through collaboration in cyberspace, and a network of trusted partners in other organisations and business.

As the intelligence community looks back to 2006, it sees the revival of tradecraft as its greatest achievement, and central to the transformation process. Creativity and innovation are highly valued and rewarded. Cross-disciplinary and trans-disciplinary concepts are brought to bear on new threats. The community-wide investment in strategic analysis, especially estimative intelligence, is maintained to ensure a future-focused context for planning and decision-making.

### Scenario Two – Adaptation

In 2016, the intelligence community and the wider body of intelligence practitioners have addressed an increasingly complex threat environment by adapting practice, which has made people, processes, organisations and systems more robust in the face of change. However, the pace and effectiveness of adaptation is uneven across the wider intelligence community.

*Adaptation* was a pragmatic choice as the new threat agenda created the licence and urgency to change old models and methods in line with established conventions and protocols. For example, managing the multi-generational workplace poses challenges, and Generation Y analysts prove difficult to retain, but they do return in response to interesting new challenges faced by the intelligence community, and bring with them new perspectives from a multitude of external workplaces.

The wider intelligence community remains organisation-centric but uses inter-organisational coordination mechanisms across the wider intelligence community to provide 'sense and respond' capability, especially given the multi-dimensionality of emerging threats. Agility is provided by the emergence of 'intelligence entrepreneurs', not career intelligence officers but innovative practitioners engaged contractually on a problem-by-problem basis, and able to confidently exercise new tradecraft approaches.

As the intelligence community looks back to 2006 it sees adaptation has grown out of the community's

heritage of resourcefulness. This heritage embedded in the rapidly declining Baby Boomer component of the intelligence community is being leveraged through a strategic knowledge management program ensuring useful insights are sustained in the now dominant Generation X-Y workplace. The recognition of common challenges across the intelligence community has invigorated collaboration.

### Scenario Three – Status Quo

In 2016, the intelligence community and the wider body of intelligence practitioners have addressed an increasingly complex threat environment by lifting the tempo of operations and shifting resources to pressure points as they occur. The community retains a formidable intelligence capability but it is difficult to shape and focus that capability in a coherent way across the intelligence community.

*Status Quo* was considered the only practical alternative by an intelligence community reliant upon evolutionary change rooted in a search for efficiencies, and a pragmatic drive to get on with the job. The absence of a strategic vision for intelligence capability development has coalesced the wider intelligence community into a number of smaller fiercely independent groupings with little formal basis for cooperation, and a growing number of disincentives as fierce competition emerges for the provision of advice from government and private sources. Cooperation is limited to traditional partners, and with selected private sector providers.

Recruitment campaigns couched in traditional appeals fail to attract newer generations of intelligence practitioners, and institutional knowledge leeches away from the community with the decline of the Baby Boomers. Intelligence organisations have resorted to poaching intelligence staff from other agencies and staffs rather than modernizing their own human resource management approaches. Critical gaps appear in the intelligence value chain as unintended consequences of the poaching activities.

As the intelligence community looks back to 2006 it sees the continuity of mandates as vitally important. Mandates have lent structure to the community, providing it with a clear purpose, a hierarchy, and acknowledged limitations. Mandates have engineered the status quo. Intelligence practice remains much the same as it has over the last 50 years notwithstanding

the advance of technological enablement. Old methods and mindsets are being used in old ways, and while offering some utility, there is a strong sense of diminishing returns.

### Implications

The scenarios are differentiated on the basis of how the intelligence community sensed and responded to change in the threat environment. Emerging threat agents are aware of intelligence community weaknesses and seek to take advantage of this. However, the community must ensure that its capacity to change remains in advance of any imperative to change.

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.

Indeed, the scenarios stressed that the intelligence community 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 future-proofing of intelligence capability, especially through partnerships extending beyond the traditional intelligence community.

As new intelligence people will relate to cross-community challenges rather than organisational loyalty, accredited training will be necessary to ensure transportability of qualifications across the intelligence community. Systems standardization across the intelligence community is unrealistic; however, interoperability and complementarity are worthwhile and achievable design objectives. Innovation in tradecraft through partnerships beyond the intelligence community offers the only real sustainable competitive advantage in a dynamic threat environment.

Clearly there are powerful impediments to change, the so-called 'weight' factors, such as legislation,

institutional conflicts, and legacy systems. However, Australia's response to modern terrorism shows that sufficient political will and resources can be exercised to make bold, widespread and highly tailored change for strategic ends.

## Conclusion

The purpose of thinking about the future of intelligence is to challenge the assumptions, and as a result, make better capability development decisions in the present. The themes outlined in this Note - threat complexity, human resources, organisational change, systems development, and tradecraft – will be influential in shaping the future of intelligence but they will not prescribe it.

Likewise, the three scenarios – *transformation*, *adaptation* and *status quo* – do not represent the totality of the future of intelligence, but they offer a basis for challenging deeply held assumptions, and illustrate that decisions made by the intelligence community in 2006 about how to respond to the emerging threat environment will have far reaching consequences.

## Footnotes

- 1 The Australian Institute of Professional Intelligence Officers Inc. was founded in 1990 and is incorporated as a non-profit making organisation with the aim of promoting intelligence as a recognised profession in Australia and increasing understanding and cooperation between members and intelligence organisations and promoting the use of intelligence processes and technology.
- 2 The 'sense-and-respond' response is predicated on the idea that changes are so rapid that they outstripped the ability to foresee and plan for them. This requires that organisations need to sense changes and rapidly adapt to it rather than relying on the existing and slow-to-respond mechanisms of process redesign, top-down management change and other conventional tools.
- 3 <http://www.zdnetindia.com/news/communication/stories/159200.html> [Accessed 1 Nov 06] The U.S. intelligence community unveiled its own secretive version of Wikipedia, called Intellipedia, which allows intelligence analysts and other officials to collaboratively add and edit content on the government's classified Intelink Web.
- 4 The intelligence community is becoming more reliant on information that can be bought or acquired without cost, and adds value to existing intelligence at lower cost than by obtaining the information through classified sources and methods.