

**STRATEGIC
ANALYSIS
AUSTRALIA**

Hyper-digitised and hyper-personalised

The world has hard problems for
Australia's Intelligence community



Michael Shoebridge

October 2023

Hard problems for Australia's intelligence community

Contents

1.	The Bottom Line	2
2.	The intelligence problems of the last decade are still with us	4
3.	The new intelligence problem: who is actually shaping the world?	6
4.	Power is becoming concentrated in a tiny number of people	7
5.	Australia's assumptions about America need to change	9
6.	5 Eyes still matters, but institutional relationships are no longer enough	11
7.	China presents a different but equally difficult challenge	12
8.	Human intelligence is back in style	14
9.	Australia's national attack surface is too large for government alone	15
10.	Australia needs to ask harder questions	16
11.	AI creates a new secrecy problem	17
12.	Intelligence agencies need to challenge their own assumptions	18
13.	The intelligence community needs to be more imaginative than those it advises	19

Published by: **Strategic Analysis Australia 2026**
www.strategicanalysis.org

Author: Michael Shoebridge is founder and director of Strategic Analysis Australia. From 2018 until September 2022, he was the Director of the Defence, Strategy and National Security Program at the Australian Strategic Policy Institute (ASPI) in Canberra. Before the think tank world, Michael was a deputy in two Australian intelligence agencies – the Australian Signals Directorate and the Defence Intelligence Organisation. He has worked in two Australian Federal Government ministers' offices. As the First Assistant Secretary for Strategic Policy in Defence, he led the team that wrote Australia's 2013 Defence White Paper and also administered defence exports policy and legislation.

Note: This is an outsider's perspective on major changes to the world that confront Australia's – and many other nations' – intelligence communities. The author has a distance of ten years from time inside the walls of any intelligence agency. So this work is an open source product, making it a view from outside the machine. That has limitations and advantages.

Hyper-digitised and hyper-personalised

The intelligence challenges of the last decade haven't gone away. But the world has become faster, more digital, more personalised and less predictable – and core assumptions that previously underpinned Australia's (and other nations') intelligence community are dangerously outdated. They need to be challenged and changed.

1. The Bottom Line

Intelligence agencies have spent the past decade grappling with [profound changes](#): the explosion of open-source information, the rise of secure cloud computing, the digital [vulnerability of human intelligence](#) operations, the challenge of [quantum decryption](#) from quantum computing, and the persistent problem of seams between agencies and partners, both within countries and between them (even for the closest of partnerships).

Those problems of speed versus institutional stovepipes and seams haven't gone away. Instead they have been joined by a new set of challenges that are more consequential for the world of Australian intelligence.

Artificial intelligence is changing the nature of cyber threats, information warfare and decryption. Digital power is increasingly concentrated in a tiny number of companies and individuals.

Political power is becoming more personalised — and in key centres (notably America, but also in parts of Europe) is being less informed and shaped by the institutions that wrap around leaders. Long-standing international partnerships are fracturing. China is a major centre of digital systems and technology, as more of our physical world goes digital and becomes software-defined. The assumptions Australia has traditionally made about the United States and its intelligence relationship with us are breaking down in obvious ways that officials and ministers are [reluctant to confront](#).

People and whole nations face two digital worlds – one China-centred and one US-centred. There are no other sources of broad digital power on the planet – not in Europe or India, or even in the advanced economies of Japan and South Korea. Many governments and economies, including Australia's, are intermingling both US and Chinese digital technology, often without policy forethought for the wider consequences.

This new landscape means Australian intelligence agencies need to think hard about what they collect intelligence on, who they collect it about, and how they do so. I'm not focusing here on the lists of [intelligence priorities](#) people like ASIO boss Mike Burgess set out – non-state actors, foreign interference, cyber agents, violent extremists and terrorists, I'm looking at big new drivers and trends changing the globe and the way our economies run and our governments and its agencies operate.

China, with its authoritarian government remains a hard intelligence target, but it becomes ever more important to other nations as China's economic role and its technological power grows. What will other states accept or buy from China, and what will they refuse?

Australia is not alone in facing a United States that can no longer be treated simply as an unquestioned partner whose interests and decision-making processes can be understood through deep institutional relationships. American directions and influences must be an important subject of Australian intelligence collection and assessment, as uncomfortable as that might feel to officials and ministers.

At the same time, people such as Sam Altman, Elon Musk, Jensen Huang, Jeff Bezos and the leaders of major Chinese technology companies like Deep Seek's [Liang Wenfeng](#) or Baidu's CTO [Wang Haifeng](#), together with key Beijing government AI policy officials like [Ding Xuexiang](#), can make decisions with consequences for Australian security and prosperity that rival those of governments.

Australian government institutions, including our most technologically capable ones, are facing a world where there is a rapid loss of control of the technological frontier to a tiny number of powerful tech companies led by a tiny number of people in both America and China. And in many ways, these are a new form of insurgent 'non-state actor'.

In a hyper-digital and hyper-personalised world, human intelligence is not becoming less important or old-fashioned. Maybe counterintuitively, it's more important.

2. The intelligence problems of the last decade are still with us

The intelligence community has spent the past decade dealing with five major [challenges](#) around how it functions.

1. Sheer rate of change The world is moving faster, decisions are being made faster and political leaders have access to an extraordinary range of information from multiple sources. Intelligence agencies have consequently found it harder to provide decisionmakers with genuinely additional insight.

The problem is not a lack of information, it's that the people making decisions already believe they know what is happening and are tapped into multiple sources of their own.

The explosion of open-source intelligence has made this particularly significant. The digital world has produced an enormous volume of publicly available information, and individuals and organisations outside government are increasingly capable of using it to form sophisticated assessments. Decision makers have often made up their minds before intelligence gets to them.

That challenges a traditional intelligence mindset which can place a premium on information precisely because it is difficult to obtain. But the fact that information has been collected secretly or covertly does not necessarily make it more valuable than information that is openly available. A bigger problem is selecting what out of the firehose of information is worth focusing on and using. And what piece of fairly inconsequential information might be crucial if it's added to something another agency knows.

2. Rise of the secure cloud Intelligence agencies traditionally wanted to own and control their own digital infrastructure – services, networks, bespoke applications. The emergence of hyperscale cloud providers has challenged that model. Increasingly, highly sensitive information can be and is being hosted on secure commercial infrastructure, subject to extensive government oversight and controls.

That might still seem an edgy tech frontier to folk used to owning and operating all their own stuff, but it does create obvious advantages. It also means government agencies have had to become comfortable with a different relationship between security, technology and control.

3. Digital vulnerability of [human intelligence operations](#): Old-fashioned spying confronts a new world of digital connection. In the past, a human intelligence operative could establish a convincing cover identity around a person,

a history and a plausible explanation for their activities that would withstand expected scrutiny.

That is much harder in a digital world. A credible identity increasingly requires a digital life: years of online history, relationships, records and activity. A recently constructed identity is much easier to expose. The digital footprint and snail trail we all leave that makes modern life convenient and connected also makes clandestine activity much harder.

4. Quantum computing, particularly [quantum decryption](#) The prospect that quantum computers could eventually break existing forms of encryption has been a major concern for intelligence agencies and governments, and that concern became a global policy issue in [2019](#) with a technical breakthrough by Google's quantum computing effort.

The important qualification is that the threat has not yet become the reality once feared. That has created a race between the development of quantum computing and the development and adoption of quantum-resistant encryption.

Unfortunately for governments and companies, though, the expected timeline for practical quantum decryption systems looks to be getting [shorter and nearer](#): 2029 is the new earlier date Google has set for shifting to a completely quantum-resistant world for its systems.

5. The enduring problem of seams and stovepipes Intelligence problems rarely – never - fit neatly into bureaucratic structures. There are seams between intelligence agencies, between intelligence and law enforcement, between collection and assessment, between federal and state governments, and between Australia and its international partners.

Information can exist in several different organisations without anyone having the complete picture. The [Royal Commission](#) into the Bondi terror attack (and the attack itself) provides a stark example of why this matters. Information about individuals even government-owned and generated information – including travel, contacts, activities and what different agencies knew or did not know – can sit in different institutional repositories.

The problem is not that a government lacked information. Instead, the pieces were never assembled into a picture that led to action – until the inquiry into events happens and there is retrospective clarity.



The Bondi terror attack in December 2025 was a reminder of the sheer difficulty in preventing attacks. It also probably shows how seams between agencies create obstacles to cooperation. Image: Shutterstock.

Seams are an old intelligence problem that anyone associated with the aftermath of the 9/11 terror attack on America and the [9/11 Commission](#) that came out of it will understand. It is still insightful reading 25 years on.

But today's world makes the consequences of failing to solve the problem of seams greater, because there are more seams and there's a higher volume of data held inside each — and the data is moving faster.

3. The new intelligence problem: who is actually shaping the world?

If the challenges of the past decade were difficult, the new environment is more demanding again.

The first problem is simply information and data overload, with much of the data of questionable value. Ten years ago, it was possible to worry that political leaders were receiving too many sources of information and that events were moving too quickly for governments to keep up.

Today, the digital feeds of 2016 look almost like a relaxing, low-key luxury.

Decisionmakers face an environment in which they can struggle simply to know what has happened, let alone establish what it means or decide what to do about it. And while they are struggling to get a basic grip on a problem, new angles or problems emerge (read Prime Minister Albanese’s “headline” [speech on AI](#) made just weeks ago for an example of thinking being swamped by events).

And the subject of that ill-fated speech — Artificial intelligence — is accelerating the problem. AI is becoming a cyber actor, a producer of misinformation and disinformation and a tool for sophisticated hacking, decryption and cyber defence.

The conventional debate asks whether China or the United States will win the AI race. That’s an important lens, but it’s probably the wrong question. The more fundamental question is whether anyone – human or human-directed government actors - will control, or even fully understand, the most capable emerging AI models, how they cooperate and how they interpret their purposes and tasks.

The issue is not simply whether Washington or Beijing develops the most powerful technology and who does this the fastest.

It is what happens if anyone develops AI systems that are extraordinarily capable, potentially destructive (deliberately or almost as a byproduct of their activities) and if such models are beyond effective human control. The fact that the top AI labs seem to have prioritised growth and fast deployment (bankrolled by the largest capital investment splurge in human history) over security and control is now glaringly obvious. And extraordinarily disturbing, given the pace of growth in model capability.

The still emerging spills of information about [top US AI firms’ frontier models](#) breaching the security of governments and other tech firms, operating in groups of hundreds or thousands, and thinking through how to cover their tracks and deceive their creators, makes this a far more credible and near-term possibility than slow-moving government leaders seem to understand.

The intelligence problem is changed fundamentally.

4. Power is becoming concentrated in a tiny number of people

Another transformation that intelligence agencies have to take seriously is that technical and digital power is concentrated in a small number of companies – and a small number of individuals who run those companies.

Concentration of power in individuals is particularly striking in the United States and China. A handful of people make decisions that affect the global economy, information environment, communications infrastructure and military operations.



Individuals like OpenAI's Sam Altman, Nvidia's Jensen Huang, and Alibaba CTO Zhou Jingren are making decisions that affect our world. Image: Shutterstock.

The problem goes well beyond Silicon Valley. It is a transformation of where power resides.

Elon Musk's decisions about Starlink and its availability to Ukraine are an obvious illustration. Early in the war, [he refused](#) to give the Ukrainian government and military access to Starlink over Crimea because he personally feared Russian escalation to a broader war.

Later in the war, Musk has again decided who does and who doesn't get access to Starlink, this time by [denying Russia access](#) to Starlink to use against Ukraine. The fact this second decision is a morally correct one is welcome, but not really the point. A private businessman has been making decisions affecting the conduct of a war and the capabilities available to two nations at war. Crucial decisions may not be based on the advice or decisions of the US government – the national government with jurisdiction over Musk.

Decisions of an individual can be capricious, instinctive, considered, insightful, impulsive or naïve, depending on the moment, the issue and the individual. That

means governments are no longer the central actors in every strategically important decision.

Intelligence agencies need to adjust accordingly.

Agencies need to understand not just governments, ministers, officials, departments and military headquarters, but the individuals who control critical companies, technologies and infrastructure.

As an example, here are some questions with important implications for several governments, including Australia's.

Where and who is Nvidia's Jensen Huang considering contracting for new semiconductor manufacturing? How is he planning his efforts to sell more advanced AI chips to Chinese firms and what is his strategy for engaging with the US Administration to allow this to happen?

Where is Jeff Bezos considering locating Amazon's expanding logistics networks and data centres? Who and what is influencing his thinking?

What directions is Alibaba Chief Technology Officer Zhou Jingren taking Qwen models in both as technologies and as commercial propositions?

Where is the world's computing power moving? Are any nations in our region (Indonesia?) likely to become powerful centres of computing power and what might that mean for other measures of power in the future? Is it all about data centres or is distributed computing power also a solution?

Which hyperscale AI companies are prepared to partner with Australia and on what terms? Who is making those decisions, on what factors and with what influences?

These are policy questions and they are intelligence questions. They are also increasingly national security questions with deep economic and societal implications.

5. Australia's assumptions about America need to change

For Australia, perhaps the most jarring change is the breaking of the assumptions that have traditionally underpinned our relationship with the United States, combined with the devaluing of some of the deep connections.

Australia has built extraordinarily close intelligence relationships with the United States and the other countries in the Five Eyes network.

Those relationships remain important and continue to operate. But Australia should not confuse the strength of institutional relationships with certainty about – or even insights into – the direction of American political decision-making.

The United States that elected Donald Trump twice is not the America that Australian institutions built their strategies plans and engagement around.

The fracturing of long-standing American political and security relationships – including tensions across NATO, the US relationship with Europe, the US–South Korea relationship and even, still most extraordinarily, the US–Canada relationship – is evidence of broader changes. And Canada is a Five Eyes partner...



America is in the middle of some fundamental changes in how it engages with the world and longstanding partners, as Vice President Vance has demonstrated. Image: Shutterstock.

The rise of nationalism over multilateralism is another. The United States is driving much of this change, challenging elements of the post-Second World War order from which America benefited enormously and in which Australia built much of its own security strategy.

For Australia, that creates a difficult but unavoidable question:

What happens now that Australian and American interests no longer converge as closely as we have assumed and planned around?

The answer cannot simply be to hope that the divergence does not matter. It needs to be understood.

That means the United States itself becomes a subject of Australian intelligence collection and assessment.

That may sound jarring and it should sound disturbing. But that's what the coffee smells like. That's the new kaleidoscope pattern.

6. Five Eyes still matters – but institutional relationships are no longer enough

Australia has traditionally benefited enormously from intelligence cooperation with the United States.

The institutional connections between Australian and American intelligence agencies remain valuable.

But the US political system is becoming more personalised, while the connections between some US institutions and American political decisionmakers are obviously less predictable. Political change in other places – like [Germany](#) and [France](#) and [perhaps the UK](#) show this isn't an isolated problem, but the US has become the world leader in hyper-personalised, erratic decision making.

Understanding the United States, therefore, increasingly requires understanding the people around its political leadership as well as the formal institutions of government.

It turns out that it's not just in Russia that folk like a leader's ex-chef (the now deceased mercenary leader, [Yevgeniy Prigozhin](#)) or business pals are key figures shaping their decisions. In the current US Administration, perhaps some of the most influential voices and brains affecting what President Trump does, aside from his own instincts and judgements, have turned out to be his son-in-law [Jared Kushner](#) and one of President Trump's golfing buddies, [Steve Witkoff](#). Cabinet figures like Marco Rubio and heavyweight institutions like the National Security Council, the State Department and the Office of National Intelligence look less influential and less connected to decision making than their predecessors under every previous Administration of the last 30 years.

This is not an argument for or against intelligence cooperation with America. It is an argument for recognising that cooperation and independent assessment are not opposites – we need both. It's also an argument for recognising where influence is coming from in a system we engage with and depend upon deeply.

The old assumption that close friends do not collect intelligence on each other becomes much harder to sustain in a world where the sources and directions of decision-making are less predictable. Australia needs to know what America is doing, what America might do next, and what the drivers of decisions are.

Australian agencies need to be able to maintain intelligence and assessments that are genuinely Australian, and simply not shared with our American ally. That means Australian Eyes Only (the “AUSTEO” label) needs to become a more meaningful and larger category.

7. China presents a different but equally difficult challenge

China is becoming an increasingly important centre of digital technology, economic activity and infrastructure. Chinese-designed and Chinese-owned digital systems are present across and inside economies and governments around the world.

For Australia, this creates a growing public policy and intelligence challenge that's not limited to traditional questions about the Chinese military or foreign policy. It includes the digital systems embedded in transport, electronics, communications and the goods and services Australians rely upon.

And it is complicated by the continuing opacity of Communist China's authoritarian political system. China's government increasingly treats more aspects of human behaviour and interaction as security issues, while political control under Xi Jinping tightens.

China is one of only two ‘digital poles’ on our planet. Along with the US, it is defining and leading digital development, including AI development. It is equally possible for powerful AI models developed by Chinese companies to threaten digital elements of Australia's economy, government and society as it is for US AI models to do this. And, while the Chinese Communist Party places the highest priority on the Party being in control of all facets of Chinese life and technology, a world where the Chinese Communist Party directs powerful AI is a disturbingly malign prospect.



Chinese AI models are establishing a dominant position in key markets, including Silicon Valley, owing to their open weight approach, performance and price. Image: Shutterstock.

China is betting on “[open weight](#)” AI models that can be downloaded onto users’ computers and which can be used at a fraction of the price of US frontier models.

The Chinese strategy is leading to a [huge proliferation in downloads](#) of Chinese AI models, outpacing US competitors in key markets including Germany, Singapore – and America itself. This raises the prospect of Chinese AI dominating global markets. It also creates a growing financial pressure that can threaten the core business model of US AI firms.

That’s because these hyperscale US firms like Anthropic and OpenAI have [investment plans](#) totalling \$trillions and these have to be financed – which means they need paying customers at mass scale. Selling lower cost models to compete with cheaper Chinese alternatives is a partial solution, given the disproportionate costs structures of the big US firms.

This looks like both a commercial and a strategic issue: if Chinese AI models undercut the business cases of the high-end US AI firms, could this disable these key sources of technical advantage for the US? Is there a growing risk to the financial viability of the top US AI firms, which already have had analysts questioning their [extraordinary IPO valuations](#) and investment plans?

Similarly, what are the medium and longer term business models of Chinese AI firms to monetize what is largely an open source approach to AI? If these firms are not financially viable, how will a shake out and consolidation happen and what ownership, state interventions, financing and control structures will result?

Australian intelligence, therefore, needs to understand not just what China can do, but how decisions are actually made within China's political and technological system. That includes understanding the individuals driving China's technology and AI development.

Here are some examples of some obvious questions any Australian decisionmaker on AI and engagement with China might want to grapple with:

Who matters in the development of Chinese AI models? What might tether Chinese “open weight” AI models [back to China](#) even where these are open-source systems?

How does the rapidly growing adoption of Chinese AI models affect other aspects of our world, including economic relationships and political power?

What are the limitations and potential vulnerabilities of Chinese AI models to Chinese state intervention?

Who influences, constrains or directs the builders and deployers of Chinese AI?

What role does the Chinese Communist Party play and who are the key officials in this area of policy and decision?

What constraints and requirements for access or control does the Party impose? And where does the balance sit between commercial incentives, technological competition and political control? How effective is that political control for how Chinese AI models actually operate, including when used here in Australia?

8. Human intelligence is back in style

Consider a paradox.

The more hyper digital the world becomes, the more important human intelligence becomes.

If a small number of people can make decisions with enormous consequences, understanding those people becomes critical.

That means knowing what their goals and motivations are, who they are talking and listening to, what they are trying to achieve in the near, medium and longer term, where they are investing, and what – and who - influences their decisions.

It means understanding the people behind the technology.

In the United States, that could mean people such as Sam Altman, Elon Musk, Dario Amodei, Jensen Huang, Alex Karp and Jeff Bezos.

In China, it means understanding the people driving companies and technologies such as Alibaba and DeepSeek, as well as the officials responsible for China's industrial and technology policy. Names like Liang Wenfeng (Deep Seek), Yang Zhilin (Moonshot AI), Zhou Jingren (Alibaba) and Zheng Shanjie (National Development and Reform Commission) look relevant here.

This may not sound like traditional state actor and agency focused intelligence. But it is intelligence about the people who increasingly shape the technological and economic environment in which governments operate and that we all live in. And it requires a different focus, network and skills.

9. Australia's national attack surface is now too large for government alone

The hyper digital world combined with the growing speed, scale and reach of AI enabled (or just AI conducted) cyber hacks creates a novel new problem for defensive intelligence across Australian government and corporate digital systems.

The result is that Australia's national “digital attack surface” is now simply too large for defensive intelligence and cyber security capabilities to be concentrated within a small number of government agencies.

The private sector owns and operates enormous parts of Australia's critical digital infrastructure. And technology companies are defining the frontier of cyber security and artificial intelligence.

Government agencies cannot realistically expect to remain at the absolute technological cutting edge without deep partnerships with the (foreign) companies that are creating that frontier. And outfits like the Australian Cyber Security Centre and the Australian Signals Directorate might start to look like highly capable forensic teams, able to [slowly piece together](#) how a particular digital compromise happened long after the event. Meanwhile, the challenge of how to better protect and secure the national digital attack surface looks like requiring private entities

and actors to conduct their own AI-enabled cyber defence instead of looking to government for answers.



OpenAI's agent backing into the Australian Government's Medicare systems, while a low level example, exposed the vulnerabilities that exist across government and corporate systems in the world of AI. Image: Shutterstock.

There's another loss of traditional government control baked-in here. The first loss came with secure cloud computing: governments no longer own or operate all the infrastructure on which sensitive information is stored.

The second loss of control is broader: Governments no longer define the technological frontier in the digital world; they increasingly depend upon the companies that do. That is a profound change for intelligence agencies that is unfolding fast. It makes the \$9.9 billion decade-long reinvestment into the Australian Signals Directorate through Project [REDSPICE](#) that began in 2022 look dated and partial.

10. Australia needs to ask harder questions

The changing environment means Australia needs to ask uncomfortable questions. And we need to understand that our great and powerful ally may not give us complete answers on core issues. This includes questions like:

What is the [actual damage](#) to civilian, military and US infrastructure from the Iran war? What are the implications for future US presence and for security relationships in the Gulf?

How much has American military power been diminished by the [expenditure of advanced munitions](#) and the wear on aircraft and naval vessels? How long will it take to rebuild US inventories to pre-war levels?

And will the US industrial base be able to build them beyond the levels used against a middle power (Iran) in a short, intense period to levels that are credible for a major Indo-Pacific conflict, against a potential adversary such as China with far greater capacity than Iran?

Those are not merely American questions. They are Australian questions, because Australian defence planning has historically assumed that the United States will be able to supply Australia's military with what it needs, when it needs it, in a major conflict. And that is still the core underpinning of the Government's defence [strategy and investment](#) plans, as unrealistic as that sounds.

Such assumptions must be tested against the actual capacity of the US industrial base to surge to meet its own needs, and to have the additional capacity to meet allied needs, including Australia's, wherever we are in the queue at the time.

Similar questions need to be asked about China's and Russia's military industrial capacity. How quickly can their industrial bases adapt? How much of what their militaries need do they have and can they produce when they need it? How resilient are they and what industrial vulnerabilities and dependencies do they have? Who will they supply and with what?

What vulnerabilities have been exposed in the militaries of China and Russia – and America's and our own – by the lessons available to all of us from the wars in Ukraine and the Middle East?

These are precisely the kinds of questions an intelligence community should be asking before a crisis rather than during one.

11. AI creates a new secrecy problem

Another question becomes even more important.

How close are we to AI-enabled or AI conducted penetration of hitherto secure systems and how close are such models to decrypting highly protected government and corporate information? The consequences would be enormous.

The [WikiLeaks](#) exposures in 2010 demonstrated the damage that can be caused when a large quantity of sensitive information becomes available, but there were limits then to how much of that mass of information could be analysed, synthesised and understood.

An AI-enabled mass decryption of highly protected government or corporate datasets could be vastly larger and more damaging than a Wikileaks repeat.

That's because the problem would not stop with the theft and disclosure of the information. AI could help to make sense of enormous quantities of data far more effectively than humans have been able to do in the past.

The danger is, therefore, a combination of exposure and understanding. Secrets could become accessible and then they could become searchable, correlated and analysed at unprecedented scale.

The role and value of secrecy itself in affected governments would be undercut.

12. Intelligence agencies need to challenge their own assumptions

The central requirement for Australia's intelligence community and our broader government framework is therefore adaptation that is well beyond incrementalism but closer to foundational. It starts with noticing what big underlying assumptions current plans and operations depend upon, and which of these are now broken or at risk.

While that might sound straightforward, it isn't. Individuals can find it difficult to recognise and challenge their own assumptions. However, if this is hard for individuals to do, institutions and bureaucracies find it much harder.

Large organisations develop established ways of understanding the world. They build structures, careers, processes and capabilities around those assumptions.

Changing them can be uncomfortable and requires overcoming inertia, complacency, careerism and process and behaviours that are hardwired into organisations and the people in them in the form of business-as-usual.

The intelligence community cannot afford to assume that the future looks like the past.

The assumptions that need testing include the role of governments, the durability of alliances, the importance (and growing limitations) of institutional relationships,

the value of secret information compared with open-source information, the location of technological power and the role and priority of human intelligence.

The intelligence community needs to be willing to identify cherished assumptions and throw them away when the evidence says they no longer work.

13. The intelligence community needs to be more imaginative than the people it advises

The world now is hyper-digitised but it is also hyper-personalised.

Power is increasingly concentrated in a small number of individuals and companies, while the institutions, rules and behaviours that previously provided predictability are becoming less reliable.

An uncomfortable environment confronts intelligence agencies.

They need to understand a United States whose interests converge less with Australia's than they have over the decades reaching back to World War II. They need to understand:

- a China whose technological power is growing while its political system becomes more opaque and centralised. And assess the implications of Chinese digital technologies becoming woven throughout our Australian economy.
- artificial intelligence as both a technology and a set of newly-arrived and powerful non-state strategic actors.
- where the world's computing power is moving.
- the companies and individuals building and deploying (while perhaps not controlling) critical technologies.
- how to help build defensive capabilities that they won't always own or control across a national digital ecosystem that extends far beyond government.

Most importantly, intelligence agencies need to ask questions that political and policy leaders may not yet be asking. That is one of their most important roles, because intelligence is not simply about answering the questions governments and policy makers ask. It is about identifying the questions governments and senior officials should be asking but may not want to.

Our world is jarring, uncomfortable and uncertain. That makes imagination, independence and the willingness to challenge assumptions more important than ever. And once that is done, it requires a willingness to act upon the answers.



strategicanalysis.org