STRATEGIC INSIGHTS

ASPI

Devolved data centre decisions

Opportunities for reform?

155

A report on the unintended consequences of government data centre procurement arrangements

ASPI
AUSTRALIAN
STRATEGIC
POLICY
INSTITUTE

Gill Savage and Anne Lyons

Executive summary

In this paper, we discuss current arrangements followed by Australian Government departments in engaging data centre services providers. The paper is intended to shape a better conversation on issues, challenges and factors to consider relating to arrangements for the provision of outsourced data centre arrangements.

Despite the intent of the Digital Transformation Agency (DTA) Data Centre Facilities Supplies Panel,[1] current panel arrangements place a heavy onus on individual departments and agencies to identify and mitigate data centre risks in the absence of whole-of-government oversight. This limits the opportunity to respond in a coordinated manner to wider interests of government, including concerns relating to supply-chain and concentrated data holdings.

Over the five-year horizon, clearer conversations and greater confidence are needed, particularly in relation to controlled ownership.

Image: iStockphoto/monsitj.

December 2020

While the unintended consequences of current arrangements are discussed in some detail, aspects relating to sovereignty, critical infrastructure and 5G network ownership are flagged as areas needing further consideration in the context of outsourced data centres.

This paper highlights a number of critical issues for consideration and resolution, including the following:

- Whole-of-government overview and management of data security are fragmented. The absence of a single entity accountable for whole-of-government data centre outcomes results in increased data risk, the perpetuation of market distortions and reduced market flexibility.
- Accountability has been pushed down to the departmental level. Given the limited resources of small and medium-sized agencies, this drives the selection of convenient options, which in turn establishes barriers to taking advantage of market flexibility and efficiency.
- While the mandate of the DTA is to provide policies, standards and guidance, it lacks resources and the authority to drive whole-of-government ICT outcomes.

This paper gives an overview of the current state, the unintended implications of the panel arrangements and the resulting challenges.

In addressing these challenges, it will be important to respond at two levels:

- Adequately mitigate the risk that's caused and amplified by the aggregation of data centres.
- Establish oversight accountability, including a strategy for the management of Australia's information and data assets as a whole, going beyond the current agency-by-agency approach. Such an authority would have objectives relating to data security, management of overall data risks as well as promotion of market flexibility and efficiency.

1. The current state

In this section, we focus on current data centre outsourcing arrangements and discuss the intent of those arrangements and the consequences of those arrangements in 2020.

A data centre stores computer systems and associated components, including backup power supplies, redundant data communication connections, environmental controls (such as air conditioning and fire suppression) and security devices.[2] As an outsourced service, it can be stand-alone space rental, with clients buying and managing their own services, or a managed service in which servers are provided, along with 24x7 system support and other systems management.

Data is essential to government functioning

Data has been referred to as the 'new oil' or 'new gold', but it's more than that. Most organisations can't function without it. In 2015, the Australian Government Public Data Policy Statement recognised government data as 'a strategic national resource that holds considerable value for growing the economy, improving service delivery and transforming policy outcomes'.[3] It isn't just the systems and infrastructure that are valuable and need protecting—it's the data itself:

> Data has become critical to all aspects of human life over the course of the past 30 years; it's changed how we're educated and entertained, and it informs the way we experience people, business, and the wider world around us. It is the lifeblood of our rapidly growing digital existence.[4]

That applies equally to government. Data held by Services Australia is used to make accurate and reliable payments to Australians, and Bureau of Meteorology data gives us our weather reporting and forecasts. Important decisions are made by and on reliable, trustworthy and accurate information created from accurate and reliable data.

Government data creation, collection, storage and analysis has grown and continues to grow, as does government reliance on it. With continued government policy directions promoting increased outsourcing of data storage, processing and cloud storage, the value and protection that disaggregation and diversification generate may be lost in the absence of appropriate oversight.

Overview of the panel arrangement

The Digital Transformation Agency (DTA) Data Centre Facilities Supplies Panel was established as part of the Australian Government Data Centre Strategy 2010–2025 following a review of the government's use of ICT by Sir Peter Gershon.[5] The Gershon review recommended that the government:

> Develop a whole-of-government approach for future data centre requirements over the next 10 to 15 years in order to avoid a series of ad hoc investments which will, in total, cost significantly more than a coordinated approach.

Therefore, the strategy had the following aims:

- for agencies to adopt, as soon as is practicable, modern technologies and practices that will improve the effectiveness and efficiency of data centre use
- for government data centre sites and services to be shared in ways that reduce the duplication and unnecessary cost of base infrastructure
- for government data centre sites to optimally match the business needs and requirements of the agencies; only those systems that have a genuine business need to operate on a 24/7 basis should be located in expensive, high-end data centres.

The business case for establishing the Data Centre Facilities Supplies Panel was based on analysis that an estimated cost of $1 billion could be avoided by developing a data centre strategy for the next 15 years.

The strategy outlined the key elements of the panel, including the following:

- Data centre requirements will be 'planned, procured and managed on a whole-of-government basis'.
- Data centre facilities and services will be available via a whole-of-government panel.
- Participation in the whole-of-government approach for departments and agencies operating under the *Financial Management and Accountability Act 1997* (superseded by the *Public Governance, Performance and Accountability Act 2014*) is to be mandatory.

Trigger points for agency transition into the panel arrangement are:

- lease expiry
- outsourcing contract expiry
- major asset replacement
- building move
- end of life of an 'in-house' data centre
- significant increase in data centre capacity.

The panel arrangement included and specified that:

> Portfolios, groups of agencies and large agencies which have aggregated demand above a level of 500 square metres will use the panel arrangements to acquire government data centre sites facilities and services. Smaller agencies will participate in aggregated arrangements, coordinated by Finance, to enable them to achieve the required efficiency.

The performance measures for the panel are framed as 'cost avoidance measures':

- increased efficiency in use of electricity
- reduced data centre floor space and associated costs
- increased efficiency of data centre ICT assets
- improved matching of data centre ICT facilities to business needs
- standardised ICT infrastructure architectures and earlier use of new technologies.

Notwithstanding the emphasis on cost avoidance, all providers participating in the panel have demonstrated that they're able to meet the required standard for data centre security.

In addition, the strategy specified:

> Data centre facilities and services will be acquired commercially using a whole-of-government process led by Finance. Data centre facilities and services will be sourced under the Commonwealth Procurement Guidelines in accordance with the value for money principles. Data centre facilities and service providers will become members of the panel upon meeting financial, contractual and technical conditions.

While 15 companies are represented on the panel, there's been an unexpected concentration of government procurement over its 10-year life. Analysis by ASPI of current data centre contracts published on AusTender found that, of the 87 current data centre facilities contracts with Australian Government agencies, 54% were with one data centre provider. Those contracts combined totalled $779 million in value. Contracts with the dominant provider totalled $620 million, or 79%. The next largest providers by value were $32 million (4%), $28 million (3.6%) and $14 million (1.7%).[6]

It should be noted that those figures don't reflect data volume, data value or the entire market, as some agencies operate their own data centres or a combination of insourced and outsourced centres. However, it's probably reasonable to assume that there's a correlation between the dollar value of the contract and the data volume.

The Data Centre Facilities Supplies Panel is due to expire in June 2021, by which time the DTA would need to extend the current arrangement or establish a third iteration of the panel. No information on date, changed requirements or approach has been released. However, ASPI's analysis found that most current contracts expire beyond the current panel end date. While that lessens the impact, and urgency, of any changed panel arrangements, the consequences of the current aggregation of data continue.

Concerns related to the government's ICT procurement arrangements are well documented. For example, the 2017 DTA *Report of the ICT Procurement Taskforce*[7] identified three impediments to improving ICT procurement across government:

1. lack of centralised policies, coordination, reporting, oversight and accountability arising from more than 20 years of devolved agency decision-making
2. limited capability and the risk adverse [*sic*] nature of the Australian Public Service with a focus on compliance, a fear of failure, poor collaboration and industry engagement
3. practices that do not reflect contemporary procurement best practice or support innovative technology choices, with existing systems firmly rooted in the bespoke and waterfall models of the past, and not the agile, consumer technology models of the present.

However, the report's recommendations and the government's response to the recommendations[8] didn't address data centre procurement, which has similar risks to those identified – notably around limited capability concerning ICT procurement in small to medium-sized agencies. Such difficulties would be amplified in agencies where there is inconsistency in the preparation and assessment of tenders, lack of transparency and consistency of decision-making, and poor understanding of data centre market costing models.

The impact of the panel

The data centre panel arrangements were intended to ensure a 'more efficient and effective use of data centre ICT' that, in turn, would 'deliver better services and at lower costs than would otherwise have been the case.'[9]

While it did achieve some positive objectives, including more cost-effective data centre procurement, more standardised rates and lower costs for the Australian Government as a whole, an unintended market failure has occurred in the form of:

- the concentration of providers, demonstrated by 54% of contracts being awarded to one provider representing 79% by dollar value—the cumulative effect of concentration could result in providers departing the market
- the aggregation of data holdings in data centres managed by the one provider and, as a result, a higher risk of potential single points of failure which have the potential to prevent government from delivering its services
- aggregation that fosters lack of diversification in providers, which has the potential to reduce innovation compared with a broader multi-vendor environment
- barriers to exit, given the high cost associated with moving to an alternative data centre provider, stifle opportunity and reduce market flexibility—this in essence establishes a conflict with competition policy outcomes
- the expansion of contract scope, in which new business is added to existing contracts in the absence of open market approaches.

The emphasis on cost savings has potentially had the opposite result (see box). For example, if we use a benchmark average cost of $1 per kilowatt, contract 'add-ons' can inflate the cost significantly. Unless additional new business is identified separately, the cost of hosted services will become increasingly difficult to identify, quantify and forecast.

Of greatest concern is that the panel arrangement, in the absence of whole-of-government oversight and governance, has been driven by individual agency decision-making. That has resulted in cumulative undesirable outcomes, fostered the adoption of convenient options, and most importantly has transferred whole-of-government risk to the agency level (see box). The Commonwealth Risk Management Policy requires agencies to consider their role in managing shared or cross-jurisdictional risks,[10] but that aspect isn't a prominent feature in data centre procurement.

5G: an example of inadvertent contracting outcomes

In August 2018, the Turnbull government introduced telecommunications sector security reforms (TSSRs), which were designed to guide Australia's security agencies and industry to share sensitive information to telecommunications networks. The TSSRs place obligations on telecommunications companies to protect Australian networks from unauthorised interference or access that might prejudice our national security.[11]

Those arrangements were introduced in response to the 'significantly different' network architecture of 5G and the challenges increasingly being faced by carriers in maintaining the security of customer data. The focus of concern was the potential for 5G providers such as Huawei to be subject to direction for security or intelligence purposes through legislation in their home country.

Before the implementation of the TSSRs, individual departments and agencies were, and continue to be, responsible for ensuring the security of their data held by outsourced service providers, despite the difficulties associated with identifying third-party providers and ascertaining the ownership of the contracted services.

The data centre market

The data centre landscape has changed rapidly and dramatically since the inception of the Data Centre Facilities Supplies Panel in 2010. As data creation and use continues to grow, along with cloud services, the internet of things, machine learning, artificial intelligence and data-driven industries, so too does the market for data centres.

A Frost Industry Quotient (IQ) report into Australia's data centre market reported a 20% growth in data centres from 2016 to 2017. That trend was expected to continue, driven by cloud vendors such as AWS, Azure and Google boosting demand, the Australian Data Centre Strategy 2010–25 adopting a whole-of-government approach and moving from government-run data centres to third-party, multi-tenant data centres, the rollout of the National Broadband Network, and an increased demand for cloud computing and higher performance computing applications.[12]

In contrast, and taking into account the impacts of Covid-19, Gartner predicts that the Australian data centre market will grow by 6.5% in 2021, rebounding from a 10.3% decline in 2020.[13]

There are predictions of data increasing exponentially over the next five years; the International Data Corporation suggests an increase of 125 zettabytes in 2025, up from 4.4 zettabytes in 2013.[14] With data centre demand rising at the same or even a higher rate as organisations move to the cloud, the question will be whether the data centre market can keep up with demand.

CBRE has assessed the total fitted occupancy for Sydney in 2020 as 'strong at 93%, while overall occupancy (including shell capacity) is 73%'. In addition, 'upcoming supply over the next three years is approximately 290 MW however pricing is expected to remain flat due to large upcoming retail and wholesale supply of 140 MW scheduled to come online in 2020.'[15] As such, future data centre demand is expected to be met.

In addition, current interest in data centre investment by managed funds investors is likely to ensure that capacity will meet growing demand.

2. The problem

The fragmentation and continued devolution of government procurement[16] and responsibility for cybersecurity and physical security have created an unnecessary vulnerability for government data, which is increasingly being managed in outsourced data centres.

There's a lack of oversight and management of government data security on the whole-of-government level.

The problem's creation can be directly linked to the cumulative impact individual agency decision-making in both ICT procurement[17] and security assessments and actions, without sight, or the ability to understand, asses and manage, whole-of-government implications and risk.

This is exacerbated by the public sector's risk-averse culture and the focus on whole-of-government ICT (the technology and its application), rather than whole-of-government data, which is seen as an 'interesting notion' rather than an asset (see box).

Are there issues of sovereignty to consider?

While the DTA is providing useful frameworks and guidance for departments and agencies, it can't mandate approaches and it doesn't have the resourcing to actively oversee the adoption of frameworks by departments.

The information contained in this paper points to a need to broaden the debate. The DTA has acknowledged the need to consider risks to data sovereignty, data centre ownership and the supply chain in response to emerging challenges, such as emerging risks to the sovereignty of data held in Australian Government data centres (including handling of data across borders), and increasing risks to the sovereignty and security of the hosting supply chain.[18]

The outcomes needed in this changing environment are surety, transparency and confidence of controlled ownership in the five-year horizon.

Transfer of risk

The current panel arrangement is transferring whole-of-government risk to agencies despite some not having adequate knowledge, budget or expertise to manage these risks. The focus on individual agency risk means that agencies will choose convenient options regardless of any compound risk that may be occurring across government. This is a blind and dangerous outcome.

So, who has responsibility? Currently, there is no single accountable entity.

The checks and balances in procurement policy don't address this gap. Nor do the Protective Security Policy Framework,[19] the *Australian Government information security manual*,[20] the Australian Data Commissioner's mandate,[21] Australia's Cyber Security Strategy 2020,[22] the DTA,[23] the Critical Infrastructure Framework, or any other agency or policy in the information and security space.

Risk shouldn't be outsourced, but that's exactly what's happening in relation to outsourced data centres. And it will happen increasingly with the move by government to cloud and hybrid services in which, a provider meets the required standards, then the agency is assured that its individual risk is mitigated.

Case study: The dominance of Microsoft

The issue of market dominance isn't new.

Microsoft founders Bill Gates and Paul Allen created the dominant US tech company through their unique leveraging of their operating systems' licence agreements. In its original deal with IBM, Microsoft embedded an arrangement in the contract that in effect blocked all other operating systems on the market, creating an enormously profitable monopoly. By blocking all competitors, Microsoft software became the new standard adopted by corporate America and eventually Australia.

By the late 1980s, Microsoft was the world's largest personal computer software company. A second Microsoft monopoly was formed when Microsoft Office came pre-installed on PCs and was again adopted as the corporate standard. It wasn't until antitrust cases found Microsoft guilty of illegally maintaining its monopoly that the Justice Department forced the company to compete fairly. Without barriers to entry to ensure market domination, Microsoft was forced to innovate in new markets in which it did not prove competitive.

Australian Government agencies not only accepted but embraced the Microsoft monopoly.

Devolution

The problem of devolution of decision-making isn't new. The overriding trend during the 1990s was to devolve responsibilities to agencies. That continued in a modified form into the early 2000s.[24]

However, the underlying policy direction by successive governments for ICT procurement and information security, as well as diminishing agency budgets, is having the real impact.

The 2017 *Report of the ICT Procurement Taskforce* found that 76% of the Australian Government's then $6.2 billion ICT expenditure was by five agencies: the Department of Defence, the Department of Human Services (now Services Australia), the Department of Immigration (now part of the Department of Home Affairs), the Department of Foreign Affairs and the Australian Taxation Office; 99 agencies accounted for the remaining 24%.[25] These 99 agencies have varied levels of capability and expertise to assess the issues and risks in different data centre providers' market offers. One effect flowing from this appears to be that agencies have found 'comfort in numbers' when choosing panel providers. That's not surprising given that agencies no doubt consult each other as part of making their choices.

Those percentages are likely to reflect today's breakdown of expenditure—even more so when including the Department of Home Affairs into the mix, and the breakdown of expenditure and the amount of Australian Government data in outsourced data centres. The 2017 report also recognised that the devolution of decision-making was an issue due to inconsistencies and a lack of centralised policies, coordination, reporting, oversight and accountability arising from more than 20 years of devolved agency decision-making.[26]

Other contributing factors

Demand for security expertise and capability means that many agencies, other than the five larger agencies, are struggling to keep up with the ever-increasing digital and data-centred world. Despite best endeavours, that's the current result of the way governments have dealt with complex issues, exacerbated by ongoing agency budget pressures.

This has never been more evident than with the market aggregation and lack of diversity arising from the data centre facilities service provisions. While the government has attempted to encourage competition through the Data Centre Facilities Supplies Panel, the opposite has occurred, with the result being aggregation and a dominant supplier providing the majority of Australian Government outsourced data centre facilities and services. In addition to the concentration risk, a dominant supplier also means a potential reduction in competition, as other providers may withdraw from what is a high-value, high-exit-cost government sector market.

The Australian National Audit Office's recent performance audit of Services Australia's system redevelopment found that Services Australia had maintained critical backup data capabilities in two data centres in close proximity to each other, increasing the vulnerability of the system to location-specific or provider-specific risk.[27] While those risks were mitigated and controlled by the agency, they apply equally to Australian Government agencies as a whole, highlighting a far greater risk due to the potential number of agencies and amount of data, with no whole-of-government mechanisms to review, mitigate or control risk.

Whole-of-government approaches to date

There's a confused and inconsistent approach to data protection and management across the Australian Government, caused by the plethora of information, data, cyber and security protocols, strategies, policies, frameworks, legislation and agencies involved.[28]

Many have whole-of-government oversight, but in very specific areas, and none looks at the compound risk of devolved decision-making on data and its protection (see box). This siloed approach has further exacerbated the implications for agencies that, put simply, don't know what they don't know.

Is individual agency decision-making a critical infrastructure issue?

A key objective of Australia's approach to critical infrastructure resilience is the identification, analysis and management of cross-sectoral dependencies. An unintended consequence of the lack of focus on cross-sectoral dependencies, in particular those arising from combination of multiple individual agency decisions, is the aggregation of government data in a small number of data centres in a reasonably small geographic area. While a catastrophic data incident is unlikely, it is possible. So, is data aggregation a critical infrastructure concern? In a system that's well managed, a catastrophic incident is very unlikely to occur, but what if it did?

While data centres weren't included in the original Security of Critical Infrastructure Bill 2017, Australia's Critical Infrastructure Framework is currently being expanded to include data and cloud services, including data storage and processing, along with communications and the financial and grocery sectors, through amendments to the *Security of Critical Infrastructure Act 2018*, for which consultations closed on 27 November 2020.[29]

The Critical Infrastructure Framework provides a possible home for efforts to address the global and compound risk of devolved decision-making by government agencies. While it's very industry focused, the Trusted Information Sharing Network (TISN) does have the Commonwealth Government Sector Group. The proposed legislative changes significantly expand the framework and create new powers to impose additional cybersecurity obligations on assets considered to be 'systems of national significance' and to direct owners and operators of critical infrastructure to provide information or act in response to cybersecurity incidents.[30]

There have been several attempts over the years to guide and implement a whole-of-government approach to ICT procurement. The latest was the establishment of the DTA, which has responsibility for development frameworks and guidance and managing an ICT Procurement Portal, the purpose of which is to improve the Australian Government's digital services and provide oversight of significant ICT and digital investment.[31]

Whole-of-government overview for this issue could be provided by the Protective Security Policy Framework which has centralised reporting to the Attorney-General's Department and requires agencies to identify and report shared risks and collaborate, particularly in relation to impacts on other agencies.[32]

The Department of Finance's Commonwealth Procurement Rules encourage diversity, through non-discriminatory practices and competition, by requiring a percentage of government expenditure and contracts to be allocated to small and medium-sized enterprises.[33] The purpose of the rules is to ensure accountable and transparent decision-making and achieve value for money by individual agencies and collectively in the expenditure of public monies.[34]

The Australian Data Commissioner is focused on the effective exploitation and use of government data, the Office of the Privacy Commissioner on privacy and freedom of information, and the National Archives of Australia on the effective management of government data and information. Those entities manage overarching whole-of-government policies, have a responsibility for collective outcomes and results and have a role in compliance, but decision-making rests with individual agencies.

The recently released Australia's Cyber Security Strategy 2020 proposes centralising the management and operations of a large number of networks run by government agencies, with a possible hub model, which could provide an opportunity for greater consistency and coordination in the data centre space.[35]

Under its whole-of-government hosting strategy, the DTA has announced that it will establish a 'digital infrastructure service', which will include a certification framework and governance model to address supply-chain and data centre ownership risks.[36] The yet-to-be-released strategy represents an opportunity to provide governance and oversight of whole-of-government data risks through some simple mechanisms.

To be effective, those mechanisms will need to be well thought through and determine where responsibility and costs for this compound risk lie.

3. Conclusion

There's constant friction between devolved, individual decision-making and decision-making for the collective good. Liberal democratic governments of all persuasions continue to grapple with this, as does society as a whole. The pandemic is a recent example where the cumulative effect of multiple individual decisions to abide by or breach social distancing and hygiene rules really matters, and where simple devolution without overall system oversight and management would not make sense.

In the case of data centre facilities holding and managing increasing volumes of government data and the potential and real risks arising from concentration with a single dominant provider, there's a need to consider and address the unintended consequences of what, in some important if narrow way, has been a successful approach to outsourcing. The compounding effects from having a dominant provider seem likely to grow as more cloud services and functions are bundled with, or accessed through, specific data centre providers.

To prevent a possible, but unlikely, catastrophic event involving the destruction or compromise of, or simply disrupted access to, important government data, that's essential to the effective functioning of government, questions needing further clarification are:

- Who is accountable and who is responsible for assessing and mitigating the whole-of-government effects of data aggregation in a single or small number of data centre providers?
- How is the risk assessed at the whole-of-government level, while maintaining a flexible, accountable, open and efficient marketplace?
- What is the cost and who bears it?
- How does government stay informed and relevant in the rapidly changing data landscape, particularly during a period of adoption of cloud infrastructure and services?

It will be important to address this issue at two levels:

- Adequately assess and mitigate sectoral and cross-sectoral risks caused and amplified by the aggregation of data centres.
- Establish oversight accountability, including a strategy for the management of Australia's information and data assets as a whole, going beyond the current agency-by-agency approach.

Data and information management need to be elevated to the level at which government finances are managed to ensure top-to-bottom understanding of the implications of data centre procurement decisions.

Notes

1 Digital Transformation Agency (DTA), 'Buying data centre space and services', Australian Government, November 2020, online.

2 Frost & Sullivan, 'Frost Industry Quotient (IQ)—Australia data centre service providers, 2018', 2018, online.

3 Australian Government, 'Australian Government Public Data Policy Statement', November 2020, online.

4 International Data Corporation, *Data Age 2025: The evolution of data to life-critical, don't focus on big data; focus on the data that's big*, 2017, online.

5 Australian Government Information Management Office (AGIMO), *Australian Government Data Centre Strategy 2010–2025*, Department of Finance and Deregulation, July 2013, online.

6 Analysis based on all current Australian Government procurements as at 30 June 2020, defined as data centre and/or data storage, for all Australian Government departments and agencies. For more information, see Australian Government, 'Senate Order, entity reports for complying with Senate Order on Procurement Contracts and use of Confidentiality Provisions', November 2020, online.

7 DTA, *Report of the ICT Procurement Taskforce*, Australian Government, May 2017, online.

8 DTA, 'Government response to the taskforce report', Australian Government, 23 August 2017, online.

9 AGIMO, *Australian Government Data Centre Strategy* 2010–2025.

10 Department of Finance, *Commonwealth Risk Management Policy*, Australian Government, 1 July 2014, online.

11 Scott Morrison, Mitch Fifield, 'Government provides 5G security guidance to Australian carriers', joint media release, 23 August 2018, online.

12 Frost & Sullivan, 'Frost Industry Quotient (IQ)—Australia data centre service providers, 2018'.

13 'Gartner forecasts Australian data centre infrastructure spending to grow 6.5% in 2021', *PR Wire*, November 2020, online.

14 International Data Corporation, *Data Age 2025: The evolution of data to life-critical, don't focus on big data; focus on the data that's big*.

15 CBRE, 'Asia Pacific Data Centre Trends', 2020, online.

16 Department of Finance, *Commonwealth Procurement Rules*, Australian Government, 20 April 2019, online.

17 DTA, 'ICT procurement', Australian Government, November 2020, online.

18 DTA, 'Hosting strategy: overview', Australian Government, November 2020, online.

19 Attorney-General's Department, 'The Protective Security Policy Framework', Australian Government, November 2020, online.

20 Australian Cyber Security Centre, *Australian Government information security manual*, November 2020, online.

21 Office of the National Data Commissioner, 'About us', Australian Government, November 2020, online.

22 Department of Home Affairs, *Australia's Cyber Security Strategy 2020*, Australian Government, November 2020, online.

23 DTA, 'About us', Australian Government, November 2020, online.

24 Australian National University, 'Public sector governance in Australia: system governance', November 2020, online.

25 DTA, *Report of the ICT Procurement Taskforce*.

26 DTA, *Report of the ICT Procurement Taskforce*.

27 Australian National Audit Office, 'System redevelopment—Managing risks while planning transition', performance report no. 10 of 2020–21, 24 September 2020, online.

28 Anne Lyons, *Identity of a nation; protecting the digital evidence of who we are*, ASPI, Canberra, December 2018, online.

29 Department of Home Affairs, *Security Legislation Amendment (Critical Infrastructure) Bill 2020: exposure draft*, Australian Government, November 2020, online; Tom Burton, 'Major expansion of mandatory cyber-security requirements on way', *Financial Review*, 5 September 2020, online.

30 'Major reforms to Australia's critical infrastructure laws—exposure draft legislation released', *Ashurst*, November 2020, online.

31 DTA, 'About us'.

32 Attorney General's Department, *Protective Security Framework*, version 2018.2, Australian Government, December 2020, online.

33 Department of Finance, 'Encouraging competition', Australian Government, 7 November 2020, online.

34 Department of Finance, *Commonwealth Procurement Rules*, 'Foreword'.

35 Australian Government, *Australia's Cyber Security Strategy 2020*, November 2020, online.

36 Justin Hendry, 'Govt puts its outsourced data handlers on notice', *itnews*, 29 March 2019, online.

Acronyms and abbreviations

DTA	Digital Transformation Agency
ICT	information and communications technology
PC	personal computer
TSSRs	telecommunications sector security reforms

About the authors

Gill Savage is the Deputy Director of Professional Development at ASPI.

Anne Lyons is a Fellow at ASPI.

Acknowledgement

ASPI would like to thank Australian Public Affairs for its support, without which this paper would not have been possible.

About ASPI

The Australian Strategic Policy Institute was formed in 2001 as an independent, non-partisan think tank. Its core aim is to provide the Australian Government with fresh ideas on Australia's defence, security and strategic policy choices. ASPI is responsible for informing the public on a range of strategic issues, generating new thinking for government and harnessing strategic thinking internationally. ASPI's sources of funding are identified in our annual report, online at www.aspi.org.au and in the acknowledgements section of individual publications. ASPI remains independent in the content of the research and in all editorial judgements. It is incorporated as a company, and is governed by a Council with broad membership. ASPI's core values are collegiality, originality & innovation, quality & excellence and independence.

ASPI's publications—including this paper—are not intended in any way to express or reflect the views of the Australian Government. The opinions and recommendations in this paper are published by ASPI to promote public debate and understanding of strategic and defence issues. They reflect the personal views of the author(s) and should not be seen as representing the formal position of ASPI on any particular issue.

Important disclaimer

This publication is designed to provide accurate and authoritative information in relation to the subject matter covered. It is provided with the understanding that the publisher is not engaged in rendering any form of professional or other advice or services. No person should rely on the contents of this publication without first obtaining advice from a qualified professional.

About Strategic Insights

Strategic Insights are short studies intended to provide expert perspectives on topical policy issues. They reflect the personal views of the author(s), and do not in any way express or reflect the views of the Australian Government or represent the formal position of ASPI on any particular issue.

ASPI

Tel +61 2 6270 5100
Fax +61 2 6273 9566
Email enquiries@aspi.org.au
www.aspi.org.au
www.aspistrategist.org.au

facebook.com/ASPI.org

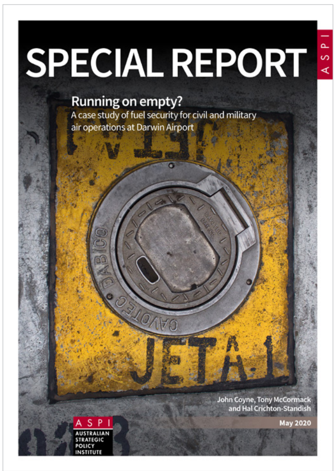
@ASPI_org

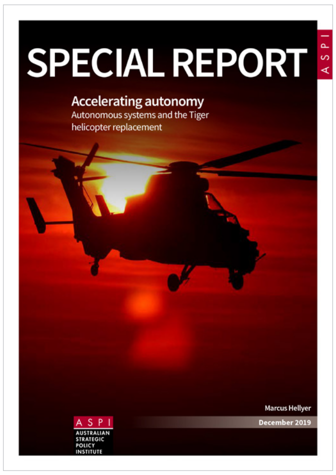
ISSN 1449-3993

Funding for this report
was provided by
Australian Public Affairs

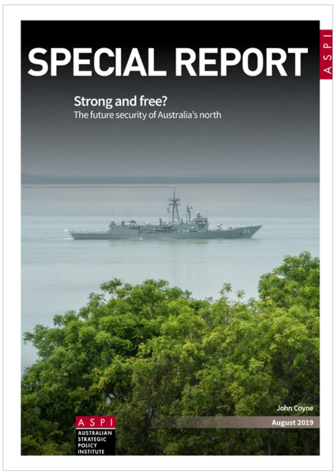
Some recent ASPI publications

After Covid-19
Volume 2
Australia, the region and multilateralism
STRATEGY
ASPI
AUSTRALIAN STRATEGIC POLICY INSTITUTE
Edited by Michael Shoebridge
and Lisa Sharland
September 2020

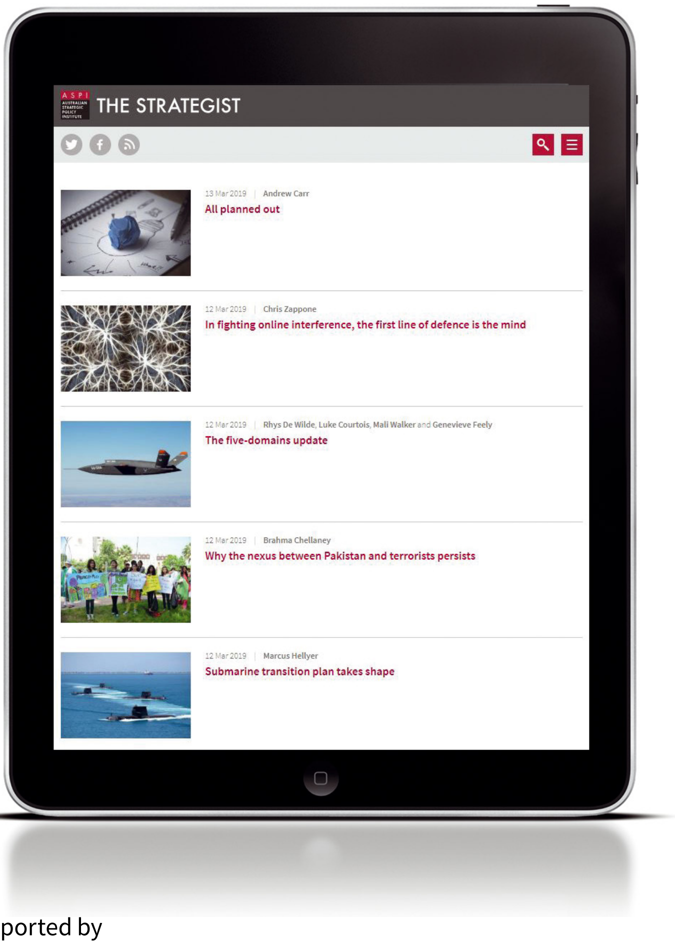

SPECIAL REPORT
ASPI
Running on empty?
A case study of fuel security for civil and military air operations at Darwin Airport
JET A-1
John Coyne, Tony McCormack
and Hal Crichton-Standish
May 2020
ASPI
AUSTRALIAN STRATEGIC POLICY INSTITUTE


SPECIAL REPORT
ASPI
Accelerating autonomy
Autonomous systems and the Tiger helicopter replacement
Marcus Hellyer
December 2019
ASPI
AUSTRALIAN STRATEGIC POLICY INSTITUTE

SPECIAL REPORT
ASPI
From concentrated vulnerability to distributed lethality—
or how to get more maritime bang for the buck with our offshore patrol vessels
Dr Marcus Hellyer
June 2020
ASPI
AUSTRALIAN STRATEGIC POLICY INSTITUTE


SPECIAL REPORT
ASPI
Strong and free?
The future security of Australia's north
John Coyne
August 2019
ASPI
AUSTRALIAN STRATEGIC POLICY INSTITUTE

WHAT'S
YOUR
STRATEGY?



Devolved data centre decisions

Opportunities for reform?

A report on the unintended consequences of government data centre procurement arrangements