STRATEGIC INSIGHTS

ASPI

Big data in national security

118

ASPI
AUSTRALIAN
STRATEGIC
POLICY
INSTITUTE

Michael Chi

Introduction

Recent developments in '*big data*' technology potentially offer the Australian national security community new capabilities that may enhance the collection, collation and analysis of information. Enthusiasm over the potential benefits of big data needs to be tempered by legislative and ethical barriers, as well as its technological and methodological limitations.

'Big data' is a catch-all term that refers to a series of concepts. On face value, it describes the rate at which data is being generated. In an era of user-generated content and social media, generating 2.5 billion gigabytes of data daily,[1] big data is growing exponentially.[2] Big data in this sense is often referred to as the series of characteristics that make it difficult to manage: volume, velocity, variety, veracity, value.[3]

In a more abstract but widely used sense, big data refers to new '*analytic*' technologies that organise and analyse large collections of unstructured data in order to discover valuable insights. It's this promise of integrating unstructured data, extracting valuable insights from it and providing new ways of predicting behaviour that has caused the widespread interest in big data.

Big data concept graphic © Warchi/iStock.

August 2017

While big data and machine learning have become buzzwords, there have been meaningful advances in both sets of technology. The use of machine learning has become an everyday occurrence, to the extent that common commercial applications of machine learning occur routinely in such diverse applications as spam and fraud detection, credit scoring and insurance pricing.[4] Over recent years, advances in big data and machine learning[5] have increasingly converged into a combined technology 'stack'.[6] This convergence has resulted in a shift in the evolution of big-data and machine-learning products from a series of individual programs towards a wider ecosystem of service provision.[7]

Given the emerging maturity of big-data and machine-learning technologies, the national security community needs to continuously revisit its assumptions about big data. This Strategic Insight provides an introduction to ASPI's *Big data in national security online resource*. This report and the online resource analyse applications for big data in Australia's national security, as well as the challenges that arise from that use. Those interested in more detail on the definitions, concepts, challenges, issues and examples in this report can refer to the online resource.

What are the applications of big data in the national security community?

In response to the growing breadth and depth of 21st century national security threats, Australian policies in these domains have emphasised breaking down 'stovepipes' to create an 'information sharing and collaboration model' underpinned by a 'need to share' culture.[8] One of the key challenges in implementing such an approach is the sheer volume or 'flood' of data. The limited capacity of agencies to manage and analyse this exponentially growing 'data flood'[9] prevents the national security community from fully exploiting its benefits. Overcoming the flood requires the application of new technologies. The national security community risks being overloaded by the information it collects if it's unable to innovate in response to the new 'big data' norm.

Integrating information

Big-data analytics technologies can potentially automate the collation of unstructured data flows,[10] making them searchable and sortable. Already, text analytics can read physical transcripts and identify relevant text—not just keywords, but concepts, sentiments, topics and people. Video analytics can similarly automatically analyse the backlog of hundreds of hours of CCTV, drone and satellite imagery feeds and recognise and track individuals automatically.[11] Fusion techniques can run across the top of these analytics and fuse different data types together automatically into an integrated feed of relevant information.[12] Such a feed can reduce the time analysts spend collating information manually.[13] A program of integration isn't a guarantee of data completeness, but it can make collating the available information a less strenuous and error-prone task.

Predictive analytics

Big-data technologies have improved the scope and accuracy of predictive analysis. In the private sector, 'predictive analytics' has become commonplace in marketing. Google Suggest builds 'models' or 'profiles' for individual users based on their search histories and other data, and then 'predicts' suggested auto-completions to search queries based on a corpus of past data, such as similar user profiles, past searches and click-through patterns—a predictive system that has underwritten Google's rise as a search engine giant. For national security agencies, big-data technologies can be used to build similar predictive models for threat and risk.[14]

Predictive analytics is not a panacea for random events or the 'unknowable future'. It relies on past data as a predictor of future performance, extrapolating functions of best fit based on past data to determine what the future is most likely to look like. It's unlikely that it will foresee inflection points beyond the data used to construct the model.

Knowledge discovery

Analysing datasets of past behaviour, or 'data mining',[15] can result in the discovery of non-obvious relationships that can be used for predictive analysis. The manual collection, collation and analysis of human-led mining for predictive insights has been the traditional cornerstone of marketing and intelligence methods.[16] Modern analytics technologies can automate and accelerate the process.[17] The increased speed and scale of analytics-driven knowledge discovery mean that algorithms can search through databases to discover correlations that previously escaped notice. Those correlations need to then be tested to establish causal or mechanistic links as part of a holistic theory-building[18] process before they can be relied on for predictive modelling.

What are the challenges for the use of big data in national security?

The use of big data in national security must overcome challenges of complexity; data quality and quantity; potentially discriminatory outcomes; and privacy concerns.

Complexity

Complexity is the fundamental challenge of big data. The analysis of big data requires the use of a pipeline of technologies, a lot of hard work from a team of multidisciplinary analysts[19] and good systems integration.[20] Investing in people, processes and technologies along this pipeline is challenging, as the complex skills requirements of big data mean that necessary workers aren't widely available.[21]

While the costs of big data are clear and daunting, the benefits are less easily expressed. Gauging the value of big-data projects ahead of time is difficult: data demonstrates value only after analysis. Data generates a 'network effect'[22] in which more data results in more potential combinations for analysis, which in turn results in more potential analytical value. The true value of any particular dataset is not clear *ex ante*, leading to a strong incentive to 'collect everything' until value is generated. This makes estimates of costs and benefits difficult, complicating planning and procurement and dulling the precision of initiatives to integrate datasets across the national security community.

In addition to project planning complexities, the complexity of the algorithms themselves has been a source of increasing concern. Certain types of algorithm have become too complex for any one person to understand or explain, no matter how much access or technical competence they have.[23] Moreover, the most sophisticated analytics and algorithms used today have tended to be the most opaque.

Data quality and quantity

Predictive analytics relies on large amounts of data. Obtaining the quantity and quality of data needed for predictive assessments in national security is challenging. Even the most accurate classification algorithms suffer from incidences of false positives and false negatives. Even with sufficient and accurate data, even the most accurate classification algorithm can suffer from occurrences of false positives and false negatives:

- False positives, or the mistaken classification of innocent people as suspicious, can arise for several reasons, such as spurious correlations,[24] overfitting,[25] or quality issues in the data.
- Conversely, false negative errors, in which a target of interest is not classified as such, present an interlinked challenge: an analyst can drive the rate of false positives to zero or the rate of false negatives to zero, but not simultaneously, and not necessarily in the same proportion.[26]

Where analytics are used in national security, there will be significant political pressure to drive the number of false negatives to zero, substantially increasing the number of false positives that need to be screened out.

Potential for discriminatory outcomes

Unfortunately, discriminatory outcomes from big-data analysis may result from biases and representation issues present in the data being used for prediction,[27] or even as a function of an analytical algorithm.[28] Uncertainty bias can affect algorithms, so that a subgroup for which there's little data receives a higher risk classification due to the increased uncertainty about its behaviour.[29] Potentially, algorithms could assess greater risk based on under-representation. There's also a risk that data analytics may be applied in areas only where the data is plentiful and available. This can also contribute to the creation of feedback loops[30] that iteratively over-target specific groups based on the increased risk generated by previous data-based decisions.

Privacy issues

Data anonymisation, or the removal of personally identifiable information from datasets, has been suggested as a way of more safely managing the use of big data. However, privacy researchers have found that even basic re-identification methods[31] have a technological and mathematical edge[32] over anonymisation methods.

In the information age, individuals are expected to accurately and reasonably gauge all the risks and trade-offs of sharing their information with a multitude of organisations. They are expected to assess the risks of their participation in an ecosystem of data sharing, assess the risks of 'downstream data use'[33] across that ecosystem, and then make a decision about whether to share their data. That decision needs to be made in a binary yes-or-no choice at the point of information collection, without a clear indication of how long the decision to consent will be considered specific, and without a clear indication of what 'reasonable' downstream uses of data might occur. The incentives for providing that consent, and the penalties for not doing so, mean that the default response has been to provide consent without reading advisory notices.[34]

Recommendations

The last national security strategy was published in 2013,[35] and the last intelligence review in 2011 indicated that 'generating insights out of the rising ocean of data' would be a key priority.[36] Australia's most recent Independent Intelligence Review has reaffirmed the importance of data analytics, management and ICT connectivity initiatives[37], and establishing governance processes to better manage technological change generally[38]. If the national security community is to effectively carry out the Independent Review's recommendations, it needs to consider the following.

Maximise the value of big data

In order to maximise the analytical benefits of big data and leverage data's networked value, the national security community will need to treat data as a strategic asset and invest in the community's big-data people, processes and technologies.

> Recommendation 1: The National Security Committee should treat data as a strategic asset and coordinate the use of big data across the Australian national security community to leverage the data's network effects.

Implementing big-data systems requires a detailed cost–benefit analysis. Methods of estimating data value *ex ante* need to be developed for the procurement and implementation of big-data solutions.

> Recommendation 2: The Australian national security community should support the development of methods for estimating the potential value of data.

Minimise the harm from big data

Methods for quantifying harm to privacy need to be developed. Research into the economics of privacy should be supported.[39] Methods for estimating and predicting the level of privacy risk that certain datasets carry need to be developed. Such methods would allow national security agencies to assess and classify the privacy risks of the data that they collect. These assessment methods will be useful in providing guidance on how to best redress privacy harm, including breaches.

> Recommendation 3: The National Intelligence Committee should work in collaboration with the Privacy Commissioner to develop analytical methods for quantifying privacy harm from big-data analytics.

Formal frameworks, processes and analytical tradecraft will be essential to minimising the risks that can come from the misuse of big data, including algorithmic errors, data issues, feedback loops, and false negative and false positive results. The imperative here is not to replace, but rather reinforce, existing analytical tradecraft with training in data science and applied statistics, and to provide knowledge of the limitations of big data to decision-makers and the wider Australian public.

> Recommendation 4: National security big-data analytic frameworks need to provide measures for accounting for false positives, false negatives and more general problems of data representativeness, bias, discrimination and feedback loops where they arise.

Manage reputational risks

The erosion of the notice-and-consent privacy management paradigm,[40] the rise of linkage and re-identification attacks on privacy, social engineering attacks and the proliferation of data are a catalyst for new privacy approaches. Australia's current privacy protections approach the level of protection enshrined in international privacy best practice,[41] such as the European Union's General Data Protection Regulation. More could be done to increase Australians' rights in line with that regulation.

> Recommendation 5: Privacy laws covering all data, not just security data, need to be updated in line with best practice.

Where algorithmic errors result in harm, mechanisms for appeal, explanation, review and redress need to be established ahead of time. This will be particularly challenging due to the tendency of people to lose trust in automated systems faster than trust in humans,[42] and maintaining such messaging to mitigate reputational harm will prove particularly challenging in the national security decision-making environment. A public-facing court, relevant to national security, would be suitable for governing such a mechanism of appeal.

> Recommendation 6: Where data-based decision systems may produce a harmful outcome, an ability to explain the process, gauge outcomes and redress harms needs to be developed.

Maintain control and integrity over big data

Providing algorithmic explanations is no simple task. State-of-the-art machine learning algorithms used in big-data analytics demonstrate a concerning and increasing level of opacity. It's unclear whether the national security community can expect a reasonable level of explicability from algorithms and analytics in the future, or what such a reasonable level of explicability would entail. To mitigate this challenge of opacity, research in the area of machine interpretability should be pursued.[43]

> Recommendation 7: Further work by both government and academia is needed to develop methods to resolve algorithmic opacity. Algorithmic black boxes cannot be permitted to become responsible for key national security decisions.

Maintaining a 'human-in-the-loop' analytics process has been proposed as an alternative solution to the opacity problem. However, it will be a costly compliance measure for a human analyst to interpret and hold to account a complex machine learning system, and, even if it's possible, it's questionable whether policymakers will be able to depend entirely upon the judgement of analysts to catch algorithmic errors on a systemic basis. However, past examples of algorithmic error highlight the importance of oversight.[44]

This is made more important by the recent discovery of adversarial techniques that can defeat or even subvert algorithms used in analytics systems.[45] Adversaries can generate 'adversarial examples'[46] using subtle but imperceptible 'fuzz', causing algorithms to misclassify objects, from stop signs[47] to malware signatures.[48] Continual bombardment with such adversarial examples can 'poison' an algorithm's training data and destroy its predictive performance. An effective audit trail and review process will be essential to detecting adversarial attacks on algorithms.

> Recommendation 8: The national security community should consider how to establish an audit and review process to mitigate adversarial attacks and data defects.

Improve data governance

The *Intelligence Services Act 2001*, the *Telecommunications (Interception and Access) Act 1979* and the *Surveillance Devices Act 2004* currently regulate the national security community's use of certain device-specific and individualised avenues of intrusion into privacy. This legislation lacks clarity, making little distinction between 'information', 'documents' and 'data'.[49] Moreover, in today's smartphone, social media and analytics driven era, any one of those warrants—telecommunications, surveillance, tracking—provides access to a much richer and interlinked body of information than in the context in which these Acts were devised. The 'structural constraints'[50] or 'transaction costs' that kept different types of data separate are no longer as prevalent. There are far fewer latent structural protections for privacy, and explicit legal protections have not taken their place.

Regardless of whether increased legal protections should try to shift this balance, there's scope to develop more clearly differentiated tiers of warrants, based on the sensitivity of information assessed as a function of the sensitivity of its content and its source, not just the device from which it was retrieved. This will be an important step as the 'internet of things' expands and more real-world information undergoes 'datafication'[51] and produces new types of data.

Providing a classification framework for data collection, similar to the classification system for retained information under the Protective Security Policy Framework, would improve data governance and public confidence by providing clearer frameworks for the audit, assurance and oversight of warranted and unwarranted data collection. The national security community's conduct in the warranted collection of data is already highly specific and individualised, as warrant applications have been noted by the Inspector-General of Intelligence and Security to be of a consistently high standard.[52] However, current frameworks for the collection and analysis of data are often viewed as a crude 'collect everything' approaches, despite the time and care that Australia's national security agencies have taken in limiting their warrant applications.

> Recommendation 9: The national security community needs to develop clearer public definitions of data and what types of data agencies are empowered to collect.

A truly integrated, oversighted and coordinated approach to big data will require a clear data governance structure in the national security community. The current structure of national security information collection and assessment would not effectively engender a data-to-decisions intelligence process across the community. Comparative intelligence scholars have noted that the Australian intelligence community is particularly disintegrative[53] and fragmented across more data silos[54] than Western counterparts.[55]

Building formal data links across these databases and silos would be an essential precursor to pursuing a wide-ranging, value-adding big-data solution for Australia's national security community. However, such a 'joined-up' approach would require a systematic review of the level of consolidation that Australia is prepared to accept in its national security community, as consolidation would notably dilute the current divide that exists between foreign intelligence and domestic security intelligence collection and use. If such a joined-up approach were deemed reasonable and necessary, organisational oversight of big-data processes and data-to-decisions cycles would be essential. This is a good case for the Inspector-General of Intelligence and Security to be empowered to provide strategic data governance across the national security community, along with the appointment of a specific Chief Data Officer.

> Recommendation 10: The national security community should have its own data custodian and data governance office within the office of the Inspector-General of Intelligence and Security.

Notes

[1] Matthew Wall, 'Big data: are you ready for blast-off?', *BBC News*, 4 March 2014, online.

[2] 'The data sources for IoT: 2015–2025', International Data Corporation, IDC Directions 2016, Vernon Turner keynote, *YouTube*, 5 May 2016, at 16:12 into the video, online.

[3] Doug Laney, '3D data management: controlling data volume, velocity, and variety', *META Group Application Delivery Strategies*, 6 February 2001, online.

[4] Solon Barocas, Alex Rosenblat, Danah Boyd, Seeta Pena Gangadharan, Laura Seaego. 'Data and civil rights: technology primer', *Data and Society*, 30 October 2014, 6, online.

[5] Matthew Mayo, 'Machine learning and artificial intelligence: main developments in 2016 and key trends in 2017', *KD Nuggets*, 20 December 2016, online.

[6] Matt Turck, ‘Firing on all cylinders: the 2017 big data landscape’, *Matt Turck VC at Firstmark*, 5 April 2017, online.

[7] Mithun Sridharan, ‘Analytics as a service: sourcing global talent on the fly’, *Wired Innovation Insights*, 19 December 2013, online; DXC Technologies. ‘Analytics as a service’, *DXC Technologies*, online.

[8] Zoe Baird Budinger, Jeffrey H Smith, *Ten years after 9/11: a status report on information sharing*, US Senate Committee on Homeland Security and Governmental Affairs, 12 October 2011, 2, online.

[9] Isaac R Porche III, Bradley Wilson, Erin-Elizabeth Johnson, Shane Tierney, Evan Saltzman, *Data flood: helping the Navy address the rising tide of sensor information*, RAND Corporation, 2014, xi.

[10] IBM Internet of Things, ‘80% of all data today is unstructured—see #Watson analyse unstructured data’, *Twitter*, 14 April 2016, online.

[11] Voula Dimitrakopoulos, ‘New data visualisation tools for the Department of Defence’, media release, Data to Decisions Cooperative Research Centre, 3 March 2017, online.

[12] Ashlee Vance, Brad Stone, ‘Palantir, the war on terror’s secret weapon’, *Bloomberg*, 22 November 2011, online.

[13] Porche et al., *Data_flood*, xii.

[14] Discovery Analytics Center, ‘Case study: forecasting the future: the EMBERS predictive analytics success story’, *Virginia Tech*, 2014, online.

[15] Mike Ebbers, Ahmed Abdel-Gayed, Veera Bhadran Budhi, Ferdiansyah Dolot, Vishwanath Kamat, Ricardo Picone, Joao Trevelin, ‘Addressing data volume, velocity, and variety with IBM InfoSphere Streams v3.0’, *IBM Redbooks*, March 2013, 3–4, online.

[16] Charles Duhigg, ‘How companies learn your secrets’, *New York Times*, 16 February 2012, online.

[17] ‘Palantir: visualising the future of crime and terrorism’, *Insider Surveillance*, 8 July 2014, online.

[18] David Bollier. ‘The promise and peril of big data’, *Report from the 18th Annual Aspen Institute Roundtable on Information Technology*, The Aspen Institute, 2010, 8.

[19] ‘Planning Committee for the Big Data Revolution: what does it mean for research?’, press meeting brief, The Big Data Revolution Government–University–Industry Research Roundtable’, National Academies Press, 14–15 October 2014, 5.

[20] Thomas H Davenport, DJ Patil, ‘Data scientist: the sexiest job of the 21st century’, *Harvard Business Review*, October 2012, online.

[21] Nicolaus Henke, Jacques Bughin, Michael Chui, James Manyika, Tanim Saleh, Bill Wiseman, Guru Sethupathy, *The Age of Analytics: competing in a data-driven world*, McKinsey Global Institute, December 2016, 39, online.

[22] Bill Schmarzo, ‘Determining the economic value of data’, *Dell EMC Infocus*, 14 June 2016, online.

[23] Jenna Burrell, ‘How the machine “thinks”: understanding opacity in machine learning algorithms’, *Big Data and Society*, January–June 2016, 1:1–12.

[24] Michael Wu, ‘The Big Data fallacy and why we need to collect even bigger data’, *Techcrunch*, 25 November 2012, online.

[25] Stephanie Yee, Tony Chu, ‘A visual introduction to machine learning’, *R2D3*, 28 July 2015, online.

[26] Committee on Technical and Privacy Dimensions of Information for Terrorism Prevention and other National Goals, National Research Council, *Protecting individual privacy in the struggle against terrorists: a framework for program assessment*, National Academies Press, Washington DC, 2008, 39, online.

[27] Solon Barocas, Andrew D Selbst, ‘Big data’s disparate impact’, *California Law Review*, 2016, 104:671–732, online.

[28] Osonde Osoba, William Welser IV, *An intelligence in our image: the risks of bias and errors in artificial intelligence*, RAND Corporation, 2017, 21.

[29] Bryce Goodman, Seth Flaxman, ‘European Union regulations on algorithmic decision-making and a “right to explanation”’, 2016 ICML Workshop on Human Interpretability in Machine Learning, New York, 31 August 2016.

[30] Fraser Sampson, ‘The legal challenges of big data application in law enforcement’ in Babak Akghgar, Gregory B Saathoff, Hamid R Arabnia, Richard Hill, Andrew Staniforth, Petra Saskia Bayerl, *Application of big data for national security: a practitioner’s guide to emerging technologies* (229–237), Butterworth-Heineman, Elsevier, Oxford, 2015, 232.

[31] Latanya Sweeney, *Simple demographics often identify people uniquely*, Data Privacy working paper 3, Carnegie Mellon University, Pittsburgh, 2000.

[32] Paul Ohm, ‘The broken promises of privacy: responding to the surprising failure of anonymisation’, *UCLA Law Review*, 2010, 57: 1701–1777.

[33] Daniel J Solove, ‘Privacy self-management and the consent dilemma’, *Harvard Law Review*, 2013, 126:1880–1903.

[34] Scott R Peppet, ‘Unraveling privacy: the personal prospectus and the treat of a full disclosure future’, *Northwestern University Law Review*, 2011, 105(3), online.

[35] Department of the Prime Minister and Cabinet (PM&C). ‘Strong and secure: a strategy for Australia’s national security’, Canberra, 2013.

[36] Robert Cornall, Rufus Black, *Independent Review of the Intelligence Community report*, PM&C, Canberra, 2011, 20, online.

[37] Michael L’Estrange, Stephen Merchant, *2017 Independent Intelligence Review*, Department of the Prime Minister and Cabinet, 18 July 2017, Recommendation 13, p.18 and Recommendation 4, p.15, online.

[38] Michael L’Estrange, Stephen Merchant, *2017 Independent Intelligence Review*, Department of the Prime Minister and Cabinet, 18 July 2017, Recommendation 14, p.18, online.

[39] James Cooper, Joshua Wright, ‘The missing role of economics in FTC privacy policy’, in Jules Polonetsky, Evan Selinger, Omer Tene (eds), *Cambridge handbook of consumer privacy*, Cambridge University Press, 2017.

[40] Office of the Australian Information Commissioner, *Australian Privacy Principles guidelines*, 31 March 2015, B.43, online.

[41] Kat Lane, ‘Review of the Information Privacy Act (2009) (Qld)’, *Australian Privacy Foundation*, 19 January 2017, 2, online.

[42] Berkeley J Dietvorst, Joseph P Simmons, Cade Massey, ‘Algorithm aversion: people erroneously avoid algorithms after seeing them err’, *Journal of Experimental Psychology*, 2014, 1–13.

[43] Zachary C Lipton, ‘The mythos of model interpretability’, *2016 ICML Workshop on Human Interpretability in Machine Learning*, New York, 16 June 2016, 96; Andrew Gordon Wilson, Been Kim, William Herlands, ‘Interpretable machine learning for complex systems’, *NIPS 2016 workshop proceedings*, Barcelona, Spain, 9 December 2016, online; David Gunnin, ‘Explainable artificial intelligence’, *Defense Advanced Research Projects Agency: program information*, 14 July 2016, online.

44 Gregory F Cooper, Constantin F Aliferis, Richard Ambrosino, John Aronis, Bruce G Buchanan, Richard Caruana, Michael J Fine, Clark Glymour, Geoffrey Gordon, Barbara H Hanusa, Janine E Janosky, Christopher Meek, Tom Mitchell, Thomas Richardson, Peter Spirtes, 'An evaluation of machine-learning methods for predicting pneumonia mortality', *Artificial Intelligence in Medicine*, February 1997, 9(2):107–138.

45 Osoba & Welser, *An intelligence in our image*, 7.

46 Nicolas Papernot, Patrick McDaniel, Ian Goodfellow, Somesh Jha, Z Berkay Celik, Ananthram Swami, 'Practical black-box attacks against deep learning systems using adversarial examples', *aarXiv*, 8 February 2016, 1, online.

47 Ian Goodfellow, 'Deep learning adversarial examples—clarifying misconceptions', *KD Nuggets*, July 2015, online.

48 Battista Biggio, Konrad Rieck, Davide Ariu, Christian Wressnegger, Igino Corona, Giorgio Giacinto, Fabio Roli, 'Poisoning behavioural malware clustering', *AISec '14*, Scottsdale, Arizona, 7 November 2014, 1–2.

49 Australian Law Reform Commission (ALRC), *For your information: Australian privacy law and practice*, ALRC report 108, 12 August 2008, paragraph 73.26, page 2484, online.

50 Harry Surden, 'Structural rights in privacy', *SMU Law Review*, 2007, 60:1605–1629.

51 Matt Turck, 'Internet of things: are we there yet? (The 2016 IoT landscape)', *Matt Turck VC at FirstMark*, 28 March 2016, online.

52 ALRC, 'Intelligence and defence intelligence agencies,' *For your information: Australian privacy law and practice*.

53 Grant Wardlaw, 'Is the intelligence community changing appropriately to meet the challenges of the new security environment?', in GabrieleBammer (ed.), *Change! Combining analytic approaches with street wisdom* (Chapter 8), ANU Press, Canberra, 2015.

54 Aaron Phillip Waddell. 'Cooperation and integration among Australia's national security community', *Studies in Intelligence*, September 2015, 59(3):25–34.

55 Sally Neighbour, 'Hidden agendas: our intelligence services', *The Monthly Essay*, November 2010, online.

About the author

Michael Chi is a research assistant and former CSC Intern at ASPI. His research interests include the policy implications of emerging technology, East Asian security, and Australia's Asia–Pacific policy. Prior to joining ASPI, Michael worked as a Research Assistant at the public policy initiative China Matters, and worked worked with HozInt, a start-up which provides a global risk and travel security alert service. Michael holds a Bachelor of International Studies (Honours) from the University of New South Wales.

Acknowledgement

This research was funded by DXC Technology, which was formed by the merger of CSC and Hewlett Packard Enterprise. The research has been conducted independently by ASPI. ASPI is grateful for the support provided by DXC. That support does not imply that DXC endorses this report or its analysis, conclusions and recommendations.

DXC.technology

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 person.

About Strategic Insights

Strategic Insights are shorter 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
Web www.aspi.org.au
Blog www.aspistrategist.org.au

facebook.com/ASPI.org

@ASPI_org