SOCIAL CYBER INSTITUTE

Research Paper 2/23

Evaluating Australian Cyber Policy Reform: Urgency, Coherence, and Depth

Greg Austin

June 2023

SOCIAL CYBER INSTITUTE

Research Paper 2/23

Evaluating Australian Cyber Policy Reform:

Urgency, Coherence, and Depth

Greg Austin

June 2023

ACKNOWLEDGEMENTS

The author would like to acknowledge comments on the paper by Professor Glenn Withers AO, co-founder of the Social Cyber Group, Director of the Social Cyber Institute, and editor of this discussion paper series.

ABOUT THE AUTHOR

Greg Austin is a co-founder of the Social Cyber Group. He has diverse international experience: as Programme Head for Cyber Power and Future Conflict at the International Institute of Strategic Studies (with offices in Singapore, London, Washington DC, Manama, and Berlin), as a Professor of Cyber Security, Strategy and Diplomacy with the University of New South Wales Canberra; and as Vice President with the EastWest Institute in its Brussels office. He has led an evaluation for the UK Cabinet Office and four other UK government departments; and has undertaken other consultancies with the UK Ministry of Defence, the European Commission, Australia's Department of Foreign Affairs and Trade, the Office of National Intelligence, and Transport for New South Wales. His academic career, including a Senior Visiting Fellowship in the Department of War Studies at Kings College London, has included eight books on international security, as author or editor. His service as a research leader for prominent NGOs, such as the International Crisis Group and the EastWest Institute, has seen him work from Brussels and London. He began his career in Australian public service roles, including posts in Canberra and Hong Kong in defence intelligence, parliamentary committees, and ministerial staff. Austin has a Ph D in International Relations and a Master of International Law, both from the Australian National University.

ABOUT THE SOCIAL CYBER INSTITUTE

The Social Cyber Institute (SCI) creates new modes of thinking specific to individual corporations, government agencies and their operating ecosystem, deploying social science insights to complement science and technology. SCI is the public research arm of the Social Cyber Group (SCG) which also offers advisory services, professional development and training. We are a Think Tank source for the well-rounded business leader.

ABSTRACT

The Australian government is preparing a new cyber security strategy to cover the period 2023 to 2030. As part of the deliberations, it called for submissions on key issues, including an evaluation framework for the new strategy. This paper responds to that call. It offers reflections on a system of benchmarking and assessment by which the strategy and its implementation can be judged. In doing so, the paper offers a critique of existing approaches as the country wakes from what the government has called a 'cyber slumber'. Three factors will be central to the success of the new commitments—a sense of urgency, a commitment to coherence between policy pillars, and investment of political capital for deep reform in individual pillars. All three factors (which we can also take as indicators of performance) depend on shared leadership by governments, industry, and community actors (especially educators). Any government strategy must be judged by its results. If there is not a visible reduction in cyber harms brought about government policy, this would appear to suggest persistent shortcomings in policy. Successive cyber security strategies (in 2009, 2016, and 2020) have not been able to show such results (reduction in cyber harms) even though the country has benefited from a visible uplift in many pillars of cyber security preparedness. Building off that discussion, the paper proposes eight principles for an evaluation framework. There should be a single overarching evaluation of the entire strategy (to ensure coherence between policy pillars) every four years as well as separate evaluations of each policy pillar, every two years. The new framework for evaluation will require much improved efforts at data collection on progress of the strategy. The data collection will need to be informed by sophisticated criteria, sustained on a continuing basis, and managed by reputable and independent social scientists experienced in public policy.

Contents

Introduction

In early 2023, as the Australian government prepares to publish its third cyber security strategy,[1] it is timely to debate the benchmarks by which the strategy and its implementation can be judged. In the preceding 14 years of cyber policy reform, the principle of commitment to evaluation of policy performance has not been accorded the high importance it should have had. In announcing a review of strategy by an expert panel in 2023, the government released a Discussion Paper which called, alongside many other things, for 'a transparent, meaningful evaluation framework to ensure the Australian Government's vision is realised, and the Strategy is fit-for-purpose now and into the future'.[2] The call for an evaluation framework is recognition by the government that existing performance assessments, like the policy ambitions themselves, have had important limitations. This paper is a direct response to the government's call for an evaluation framework. In doing so, the paper also addresses some of the shortcomings in cyber policy reform in Australia.

The paper provides comment on several questions:

- Who should evaluate Australian cyber policy?
- What benchmarks are used for evaluation?
- What is a practicable balance between qualitative and quantitative evaluation?
- What is a practicable balance between evaluating inputs, outputs, and outcomes?
- What is involved in creating an ecosystem for cyber policy evaluation in Australia?

To help answer these questions, the paper opens with a brief discussion of the benefits of evaluating cyber security policy. It then looks at the approach of successive Australian governments to evaluation of cyber policy reform as a constituent element of its overall policy agenda. This is followed by a review of several assessments or evaluations of Australian policy by different entities in the recent past.

This analysis leads to the author's conclusion that Australian evaluation efforts could usefully focus on three fundamentals as the key factors that should be central to reform of cyber security policy -- a sense of urgency, a commitment to coherence, and investment of political capital for comprehensive (in-depth) reform. All three elements depend on shared leadership by governments (federal and state), industry, and community actors (especially educators).
The paper then looks at what these three basic policy tests might mean in practice, before addressing the optimal mix of evaluation processes for cyber policy in Australia.

The paper will draw on insights from several strands of work by the author. The author has been analysing international cyber policy (mainly Russia, China and the United States), but including a focus on national cyber policy in Australia[3] for over 14 years.[4] In the International Institute for Strategic Studies (IISS) between 2019and 2023, he developed this focus on national level policy implementation assessing the cyber policies of 25 countries, including Australia, Indonesia, Singapore, China, Japan, Russia, the US, the UK, Nigeria, and Brazil.[5] He has investigated key areas of national policy in some depth, through substantial research projects on cyber security education,[6] national cyber emergencies,[7] and a substantial confidential project in 2022 and 2023 on warfighting in the information environments of the 2030s. He has also led a year-long evaluation for the UK Cabinet Office and four other government departments.[8]

Benchmarking cyber policy reform?

The value of benchmarking policy in general has been canvassed in earlier publications by this author.[9] There are at least six strong reasons for such evaluations:

- to assess performance objectively
- to create sustained pressure for improvement
- to expose areas where improvement is needed
- to identify superior processes
- to focus on the links between processes and results
- to find innovative ways of responding to a problem.[10]

Evaluation policy and dispositions for that vary sharply between countries, and even between government departments within one country. The UK approach, in place for more than two decades, is

that 'monitoring and evaluation of all proposals should be […] an integral part of all proposed interventions.[11] The UK also aims to ensure that evaluation costs should be 'proportionately included in the budget and the management plan of all significant proposals'.[12] The UK has been one of the governments most committed to policy evaluation.

There is a long history in the Australia government of commitment to evaluation[13] but the actual practice has waxed and waned. In recent years, in the planning and implementing departments, the practice has become largely moribund or lacking in independence.[14] There has been a 'general view that the state of evaluation within the APS [Australian Public Service] is poor'.[15] To correct this, and for several other reasons, the Australian government announced in April 2023 an initiative for significantly improved evaluation capabilities in government.[16]

Despite the absence of an agreed overall framework for evaluation of cyber policy, the commitment of the office of the Auditor General to performance audits over several decades, the increasing power of parliamentary committees, and a vibrant academic community have to some degree compensated for the weakness of federal government commitment to regular review processes. The Department of Industry and Resources is a clear exception to the main trend of low interest in program evaluation in Australia's civil service. In 2017, it published a four-year evaluation strategy.[17] In 2021 and 2023, it released separate evaluations of two broader government policies, inter alia, that had been set up as part of the 2016 cyber security strategy (creation of a cooperative research centre[18] and establishment of a cyber industry growth centre).

This latter evaluation of AusytCyber was highly critical, with each specific critique below applying to it and several other industry growth centres:

- poor intra- and inter-sectoral collaboration;
- poor connections between research and industry sub-optimal workforce skillsets and capacity;
- problematic regulatory issues; and
- suboptimal international connections and opportunities.[19]

Evidence of the weak commitment to evaluation within the implementing departments in Australia (at both federal and state levels) is the absence of significant budget provision for this activity, in strong contrast with their UK counterparts. The UK government has an Evaluation Task Force which 'showcases evaluation strategies' from various departments to demonstrate its commitment to reform.[20] The US Department of Homeland Security (DHS) in the USA has a variety of standing mechanisms for evaluation of its various programs, and reports on them annually.[21] The Department of Finance in Australia is the standard setter for evaluations in the Australian government, and has well developed guidelines[22] but within a permissive approach.[23]

The Department of Home Affairs (DHA), set up in Australia in 2017, has the primary responsibility for shaping cyber security strategies and evaluating their effectiveness. Its annual report of 2020 provides a useful example of the character of such evaluations in the field of cyber policy. In 2022, DHA assessed its performance in activity areas that affected cyber policy (under the overall objective of national security) against the sub-objectives and metrics set out in Table 1 below.[24] In too many places the assessments rely on the juxtaposition between 'completed in full' and 'have been progressed' or claims that activities had been completed with little assessment of the actual outcomes.[25]

The metric of success in execution was acceptance by a Cyber Security Strategy Delivery Board that 'initiatives were progressing in accordance with the timeframes approved at the Ministerial level'. Outcomes were expressed in quite generalised terms: 'increasing the public and industry's awareness of cyber security threats, coordination of Government efforts to enhance cyber security capabilities across Commonwealth agencies, expansion of Government's ability to support small and medium enterprises and individuals, and development of robust framework to protect critical national infrastructure from cyber threats'. The soundness of these claims was dramatically challenged at the end of 2022 when, in response to several large data breaches, the Minister for Home Affairs, Clare O'Neil, claimed that the country was waking from a 'cyber slumber', as also discussed later in this paper.[26]

It should be noted that the focus of this paper on evaluation of government strategies for cyber policy reform is not meant to imply that the government alone is responsible for the success of strategies,

which are necessarily based on multi-stakeholder approaches. As has been noted, 'national cyber security strategy in a liberal democracy and free market economy is not exclusively or even primarily a government-led effort. In many respects, the government can only facilitate and inspire within the constraints of tight budgets. Moreover, Australia sits in a global community of cyber security practice, technologies, policies, public education, and research on which it can draw but which it does not itself shape as an independent actor.[27] Nevertheless, governments are obliged to be accountable for the outcomes of their policies to the extent that they can control them.

Table 1: Collated List of Selected Home Affairs Cyber Policy Evaluation Metrics 2021-22

Sub-objective	Metric
Cyber Security Policy: Effective cyber security strategies, policies and advice protects and advances Australia's interests	a) Demonstrated progress against key initiatives within Australia's Cyber Security Strategy 2020 b) Enhanced national cyber security awareness for Australian families and households to protect children and vulnerable people online c) Strengthen domestic and international partnerships to ensure collective action to combat online child sexual abuse, including the organised production and dissemination of child abuse materials d) Bolster law enforcement capabilities to target, investigate and disrupt cybercrime, including child exploitation and other criminal activities on the dark web e) Enhance industry outreach and national capability collaboration to support small and medium enterprises and vulnerable Australians f) Manage technology risks to support Australian economic resilience and to facilitate economic growth g) Demonstrated progress to develop and support implementation of Australia's 10-year *National Strategy to Prevent Child Sexual Abuse*
Critical infrastructure: Effective policy development, coordination and industry regulation safeguards Australia's critical infrastructure against sabotage, espionage, and coercion.	a) Engage with 100 per cent of entities on the *Security of Critical Infrastructure Act 2018* register in relation to security and resilience b) 100 per cent of notifications received under the Telecommunications Sector Security (TSS) reforms to the Telecommunications Act 1997 are responded to within statutory timeframes. c) 100 per cent of Foreign Investment Review Board cases referred are responded to within agreed timeframes
Crisis Response: Effective all-hazards coordination and response activities enhances Australia's ability to respond to crises and critical disruptions and reduces the impact on Australia and the Community	a) 100 per cent of designated special events have a security risk plan in place b) 100 per cent of designated high office holders have appropriate physical risk mitigations in place c) Eligible non-financial disaster assistance requests are approved within six hours of an agreed request received d) Enhanced national coordination of emergency response efforts through the management of cross-jurisdictional fora
(Cyber)crime: Effectively monitor and disrupt transnational, serious and organised crime to protect	a) 100 per cent of capability plans outlining compliance with telecommunication interception obligations are reviewed within statutory timeframes, consistent with section 198 of the *Telecommunications (Interception and Access) Act 1979* b) The Department implements policy and legislative reforms to enhance responses to national security and law enforcement issues

and preserve Australia's community and our partners	c) Enhance partner governments' capability through providing capacity building resources d) Progress in implementing the *National Strategy to Fight Transnational, Serious and Organised Crime*

Australia's Patchwork Cyber Policy Evaluation System

The last decade has seen the emergence of some reasonable foundations being put in place for cyber policy evaluation in Australia. But the system might be best described as 'patchwork' rather than a system or a coherent matrix. It looks more like a set of activities cobbled together from available offcuts, rather than a logically developed and comprehensively developed analytical framework which produces clear feedback loops into policy action.

The main sources of evaluation of cyber policy in the last decade have been:

- self-reporting by individual government agencies through annual reports
- the annual sector competitiveness plan of AustCyber (an industry growth centre)
- Auditors General (federal and state)
- National Cyber Security Centre[28]
- professional associations, such as the Australian Computer Society (ACS) or the Australian Information Security Association
- Bar associations or law societies
- independent academic researchers or think tanks specialising in cyber policy
- various parliamentary committees (such as the Select Committee on Cybersecurity and Identity Theft Prevention or relevant Estimates Committees in the Senate)
- the Resilience Expert Advisory Group, CIAC
- the Industry Advisory Committee (set up by the 2020 national cyber security strategy).[29]

The reference in the preceding paragraph to auditors-general in the state governments of Australia's federal system exposes a rather large hole in claims that federal government policy, delivered by the Home Affairs Department, is working as well as it claims to make the country more cyber safe. One need look no further than the several reports of the Auditor General of the state of New South Wales criticising the sorry level of 'cyber uplift' in that jurisdiction, as recently in February 2023, to see that the Home Affairs Department annual assessments only cover the federal government's activities, and do not represent a state of the nation report card for cyber security. Australia has six states and two territories. New South Wales (whose capital is Sydney) is the wealthiest and most cyber capable state. If it is assessed by its own Auditor-General as operating below standard in cyber security, we might conclude that most of the other jurisdictions represent weak links in national cyberspace protections.

Regrettably, the moral authority, political weight, and policy remit of the various sources of evaluation of national cyber security remain highly variegated and cannot be considered to offer a coherent and comprehensive framework for evaluation. At the same time, they do present a foundation for the federal government and the parliament, along with other stakeholders, to build upon to achieve that outcome.

Evaluating 'spooky' policy

Open government in Australia, including public evaluation of program performance, has always operated in the shadows of an overriding preference of political leaders for less transparency, rather than more, a practice entrenched in law in 1914.[30] Critics will say that the country's freedom of information laws operate as a 'freedom from information' regime and were designed in that way.[31] The country has one of the weakest privacy regimes among liberal democracies[32] and on at least one occasion the national government has engaged in a secret trial, an event subsequently described by the Attorney General of the successor government as 'anathema to the Australian system of criminal justice'.[33] Its communications monitoring regimes for metadata to support counter-terrorism rules are among the most draconian in the world.[34] That report was headlined 'Australia May Well Be the World's Most Secretive Democracy'.

It is within this environment that the legitimate needs of the national security cyber agencies for secrecy have been operating. It is an environment that has not fostered public evaluation of national

security agencies or their operations with any meaningful detail. The intelligence agencies, especially ASD, have had a high degree of influence over all public disclosures and usually lean toward secrecy rather than transparency. Evaluation of the intelligence and security dimensions of national policy have a clear history of reviews,[35] in some cases in response to disaster or visible mismanagement, rather than regular evaluation as a standard operating procedure.

This tension between national security activity and less sensitive activity from the point of view of evaluation is visible in the Department of Foreign Affairs and Trade (DFAT) which has a world class approach to monitoring and review of its development programs (inherited from the former Australian aid agency that it absorbed), but which appears to have far less interest in open-source evaluation of national security programs. It published policy evaluation plans in 2022 and 2023 that did not include mention of its international cyber policy grants valued at tens of millions of dollars annually.[36]

ASD has become much more open in recent years, including through publication of a public domain annual report to government, like all federal agencies. It now publishes an annual threat report. Together these documents, and several other regular publications, have allowed unprecedented insights into its performance. The now quite regular practice of disclosing detailed information on cyber threats to help national stakeholder be better prepared and to support Allied policies of deterrence of foreign cyber attack represent quite a fundamental shift in its traditional approach to secrecy. However these disclosures do not for obvious reasons have sufficient detail to form the basis of a comprehensive judgement that the agency is performing well in protecting national cyber security.

Evaluation 2016-2020

The 2016 policy reset for cyber security set in train by the government under Prime Minister Turnbull looked promising. It included a new national cyber strategy, a Defence White Paper giving unprecedented attention to cyber capabilities, appointment of the first ever Minister for Cyber Security, a dedicated cyber security policy unit in the Department of Prime Minister and Cabinet, establishment of an industry growth centre to promote the domestic cyber security industry, and appointment of a cyber ambassador in the Department of Foreign Affairs and Trade. One of the most revolutionary and influential changes was the creation in July 2017 of a division of information warfare in the Australian Defence Force and the elevation of the Joint Capabilities Group in which it was placed to the status of a single service (such as the navy, army, or air force).

The reset certainly stimulated many enduring improvements in policy and in evaluation of it. Turnbull was the most cyber savvy member of his Cabinet, but most of his peers had little interest in the subject. There was a shortfall between ambition and follow-through. Government restructuring had a negative impact, especially the creation of a new Department of Home Affairs (DHA) in December 2017 whose massively enhanced remit would include the cyber portfolio. The momentum was further lost as a result of the failed leadership bid in August 2018 by the first DHA Minister, Peter Dutton, resulting in the elevation of Scott Morrison to the post of Prime Minister.

In 2016, several months prior to the release of the Turbull government's cyber security strategy and its Defence White Paper, I assessed that 'There has been no effort in public by the government to benchmark

Australian national security needs in cyber space in the same way as we benchmark naval, air and ground capability against strategic needs (strengths and weaknesses of potential enemies and their intentions) and against Australia's budget constraints'.[37]

Several days before the launch of the Turnbull cyber strategy, a colleague and I proposed a process to benchmark Australian cyber policy reform against that of the UK and the US.[38] In the 2016 strategy, the government committed to annual evaluation and corresponding update of its action plan but without a clear framework.[39] We followed up in May with a proposed set of benchmarks for Australian cyber policy, as set out in Box 1.[40]

However, consistent with the judgement mentioned above that evaluation in implementing departments had become moribund, the commitment in the 2016 Cyber Security Strategy to annual review was not honoured beyond perfunctory restatement of objectives with claims that the government had done more or better on almost all fronts. A 2017 external analysis from the Australian Strategic Policy Institute found that the first annual update in 2017

was 'almost devoid of self-assessment, and its approach to the review process is flawed'.[41] Moreover, in 2018, the government walked away from its commitment for annual updates of the 2016 cyber-security strategy.[42] Its reasoning seemed to be that the strategy no longer matched the operational environment, with the escalation of threats in cyberspace, including the increasing use of the information domain by Russia and China for political interference.

Box 1: Benchmarks for Cyber Policy Reform Proposed in 2016

1. Consistent articulation of the different domains of cyber security (crime, business, privacy, war); of the many dimensions of cyber security (technical, human, social and legal); and differentiated responsibilities of different sectors
2. Consistent and comprehensive articulation of the threat environment and variegated response options.
3. A comprehensive suite of governmental, cross-sector, private-public, professional, and civic organisations active in cyber security
4. National consensus on the line between sovereign capabilities and the global communities of practice
5. Effective monitoring of business and economic threats and rapid response capabilities at the enterprise level
6. Nation-wide preparedness for the unlikely but credible threat of an extreme cyber emergency
7. Effective response capabilities for social threats (crimes) against individuals, including children

One of the most useful regular assessments of progress in cyber policy to emerge came from the Australian Cyber Security Sector Growth Centre, later renamed as AustCyber, set up under the 2016 strategy with government funding. In 2017, it began to publish an annual review under the rubric of a 'sector competitiveness plan'.[43] The assessments in the first report were somewhat stark:

- Australia's system for research and commercialisation is inefficient
- the 'current market environment constrains the growth prospects of smaller Australian cyber security businesses and startups'
- a serious skills shortage is limiting the growth of the Australian cyber security industry'.[44]

However, consistent with the judgement mentioned above that evaluation in implementing departments had become moribund, the commitment to annual review there was not honoured beyond perfunctory restatement of objectives with claims that the government had done more or better on almost all fronts.

By 2020, the AustCyber sector competitiveness annual report had become far more adept at quantitative metrics and still retained a critical perspective, providing one of the best performance assessments of key areas of government policy, especially responses to the skills deficit.[45] On the other hand, its evaluative character was counter-acted somewhat by its 'cheer leader' mode of operation. (AustCyber's founding brief was to promote the growth of the sector.)

An especially persuasive set of evaluations emerged from the National Audit Office (ANAO) between 2016 and 2020.[46] One of the earliest addressed the adequacy of cyber security in the ANAO itself -- finding a high commitment to cyber security but a lack of critical review of the services which were largely provided by external suppliers: 'the ANAO does not effectively monitor the implementation of these controls, or assess the risk of known deficiencies'.[47] This audit report flagged the intention of the ANAO to expand its reviews of cyber security in Australian government agencies relying where necessary on information from key government agencies such as the Australian Signals Directorate (ASD) for guidance.[48]

The subsequent ANAO reports up to 2020 were a combination of bad and good news for the government. As summarised by Australia's ABC News, in 2018, ANAO found in a review of the cyber resilience of three government agencies they showed 'low levels of effectiveness … in managing cyber risks', following three previous audits of 11 government entities that the ANAO assessed had 'high rates of non-compliance' with government-mandated standards.[49] On the other hand, for example, a 2019 report found that the Australian Reserve Bank and the Australian Securities Commission were observing the ASD 'essential eight' strategies,[50] and that Australia Post was not. The report further found that the Bank and the Commission had 'high levels of resilience compared to 15 other entities audited over the past five years' and that Australia Post was 'not cyber resilient'. In 2020, the parliamentary Committee on Public

Audit called for more cyber security evaluations in government departments because of the continuing compliance failures.[51]

Key national security agencies (Defence, Home Affairs and Foreign Affairs and Trade) had all received negative cyber security reviews on different counts by 2020, including in the case of Defence, weaknesses in its security vetting of defence contractors for cyber security controls.[52]

In a mid-term report in 2020 on his first five years as Auditor General, the incumbent Grant Hehir, observed that cyber security of government financial systems was the area of operations that most frequently received adverse findings ('consistently identified non-compliance' with standards).[53] He further observed that 'With cyber security being an area of government priority for many years, these findings are disappointing'.

Evaluation 2020 – May 2022

Political commitment to the cyber policy reform took a new turn in mid 2020, even though Ministers in post lacked the same sort of commitment and engagement as in the Turnbull period. The 2020 reset was brought about by what the government saw as a deterioration in the country's strategic circumstances, including in cyberspace. The cyber reset in 2020 followed two clear pathways, and defence policy became its main driver.

Cyber security had moved to the centre stage of Australian government thinking about national security. This was reflected in the release in July 2020 of a 'Defence Strategic Update' which further elevated offensive cyber operations to an important role in Australia's stand-off capabilities.[54] In August 2020, Australia released a new Cyber Security Strategy[55] adopting a greater sense of urgency than its predecessors. It warned of increasing threats from other countries, and escalating risks from rapidly changing technologies and new levels of connectivity.[56]

The 2020 cyber strategy said that evaluation is important to the government and it included a short checklist of metrics for performance by government and business. [57] None of these were truly appropriate 'metrics' in any true sense of the word (a quantitative assessment for comparing performance) unless 'doing more' or 'producing more' might be understood as a credible metric.

The 2020 cyber strategy set up a new Cyber Security Industry Advisory Committee which would 'make public reports about the progress of this Strategy'.[58] This was an important advance, though not quite the same as independent and comprehensive evaluation. The strategy set 15 metrics for government, and others for industry and the community. The first annual report of the Committee in 2021 sets out over 12 pages a convincing summary of government actions against most of the metrics, but the assessments are qualitative and fairly generalised beyond stating specific government actions (such as introduction of new legislation or setting up a new organisational unit.)[59] Its approach is set out in Box 2.[60] Responsibility for evaluation of components of the strategy is assigned to the government stakeholder responsible for its implementation.

Box 2: Evaluation Approach of the Industry Advisory Committee 2022

An Evaluation Approach has been established for the Strategy, providing a framework to guide the consistent, robust, and transparent evaluation of outcomes and performance of the Strategy and its constituent components. The Evaluation Approach sets out the principles that will be applied to all evaluation activities under the framework, as well as an evaluation hierarchy that translates between the metrics and outcomes identified in the Strategy, and the more specific program level measures required to monitor the effective implementation of the Strategy. This Evaluation Approach is intended to enable Government to allocate responsibility for evaluation and reporting under the Strategy in a consistent manner, making use of existing evaluation mechanisms within agencies rather than duplicating effort. These evaluation responsibilities have also been mapped against the Strategy's governance structures, differentiating between internal Government performance evaluations, security classified elements, and public accountability of what outcomes have been achieved under the Strategy and their impact on Australia.

The second annual report of the IAC follows the style of the first one. It claimed that 'program-level evaluations continue to measure the impact and effectiveness of the Strategy's initiatives on a business-as-usual basis'.[61] It appears that this approach was the one described in text that is called out in Box 2. It also noted that the government had

advised the IAC that a 'strategic evaluation framework is being progressed in 2022 and will provide an assessment of the progress, impact and value of the Strategy'.[62]

It includes an important realisation:

> If we are to meet all of these challenges and thrive in the accelerating digital world, we are going to need to substantially uplift our cyber skills base. And we are going to need to do this right the way across the spectrum from deep cyber expertise to basic cyber hygiene practices, through our schools and universities, governments, and industry; and we are going to need to do it fast.[63]

The question arises whether the IAC had intended to offer any comprehensive evaluation of how to do that. Its 2022 report does not comment on the adequacy of tertiary education in the country for that purpose beyond mentioning some outreach or pipeline activities. It makes a very broad suggestion:

> The Department of Education and the Jobs and Skills Agency should encourage and assist Australia's educational institutions to build more basic cyber skills in a broader range of curriculums such as software engineering, robotics, and other tertiary programs. The Committee emphasised that while deep cyber specialists are important, Australia also needs to better equip a broader range of technologists.[64]

The 2022 review includes a three-page section on formal evaluation, [65] and there is clear evidence of growing determination by it and by the government to improve its evaluation. For example, in evaluating success in overcoming skills shortages, the report notes that the Commonwealth Department of Industry, Science and Resources (DISR) funded three projects in 2022 as part of a $2.5 million effort 'to improve data collection on cyber skills shortages'.[66]

The results of this effort have yet to be revealed. Moreover, measuring the skills shortage in very general terms has been one of the easiest targets for data collection in terms of numbers of graduates in the cyber security field in general at several degree levels, but further serious analysis of the impact of the shortages in any more granular detail has not been forthcoming. The efforts have also been hamstrung by underestimating the scale of the challenge.

The IAC report assesses the outputs as encouraging but mistakes them for outcomes ("the initial program outcomes indicate that Australia's cyber security posture has been significantly improved").[67] The data points the Committee cites are "outputs", not "outcomes", to use evaluation terminology, since there is little analysis of whether the threats have been reduced in any substantial way by the cited outputs.

While recognising that a more comprehensive and robust evaluation framework was needed, the IAC reports that its evaluation of the 'outcomes of government programs' were assessed against:

- the quality and quantity of stakeholder accessibility and uptake
- the reduction of harm to Australians and our national interests (the number of activities from cyber criminals which were disrupted)
- and the passage of legislation or regulatory reforms.[68]

Despite the claim in the second item that the evaluation included an assessment of a measurable reduction in cyber harm to Australia, the IAC assessment did not offer clear evidence of that.

Evaluation under a new Government

A change of government in May 2022 from the Liberal National Party coalition to the Australian Labor Party put Australia in a new position to improve its evaluation of the cyber security sector. But the unfolding of events was episodic and reactive as more negative reports rolled in and as unprecedented data breaches rocked the confidence of the Australian public in national cyber security capability.

Auditor-General

In June 2022, an ANAO assessment of critical infrastructure protection (of which cyber infrastructure is a critical element) found the Home Affairs Department had not followed through key commitments to compliance: 'The majority of policy and procedural documents (15 of 22) to support possible critical infrastructure related compliance activities were drafted, but not finalised and approved, or included in the department's policy and procedural repository.'[69] It also found that 'The

Critical Infrastructure Resilience Strategy, which guides the work of the Cyber and Infrastructure Security Centre, has not been updated since 2015, despite including a review point in 2020, and plans by the department to update it since at least 2019.'

In August 2022, the ANAO published its annual report identifying cyber security as one of three areas where government entities had regularly failed to meet expectations of good performance.[70] It observed one cause of this that is particularly relevant to evaluation: 'optimism bias in reporting by entities, and little analysis or evaluation of the success or otherwise of the policy framework'. The observation that there has been little analysis of the policy framework is an indictment of the lack of effectiveness of whatever evaluation processes have been in place. The report noted 'poor delivery of fit-for-purpose cybersecurity within the [government IT] sector'.

In a report issued on 14 November 2022, the Australian National Audit Office (ANAO) found that the Department of Foreign Affairs and the Australian Federal Police had fallen short in meeting basic standards in cyber security for supply chain assurance: 'AFP and DFAT do not manage compliance of contracted providers with the PSPF requirements for cyber security'.[71] (PSFP is the government-mandated Protective Security Policy Framework.)

AustCyber

In the 2022 sector competitiveness plan, AustCyber found that Australia is slipping off the pace in several important aspects of cyber policy reform. It identified three key challenges: limited support for start-ups, lack of access to export markets, and workforce shortages.[72] It noted that government funding for cyber security research had decreased from $9.8 million in 2019 to $7.5 million in 2022. On the skills deficit, in spite of growth, there would still be a shortfall of around 3,000 skilled workers by 2026. The report also found that in Australia, the growth of the cyber security sector had been slower than for the top nine countries by annual growth rate.[73]

Incidents speak louder than words

The change of government in May 2022 was followed by several cyber incidents on a national scale that by the end of the year would serve to puncture the complacency in the Australia's cyber ecosystem. There were two incidents of compromise of sensitive personal data in quick succession (from Optus and Medibank) that were unprecedented in the country and rocked community confidence in the country's cyber security, even if the number of citizens affected was much smaller than in similar incidents in some other countries.

On 22 September, the telecommunications company Optus reported a possible compromise of personal data,[74] and confirmed that attack two days later.[75] The response outlined by the company indicated (only on 30 September) that the personal identification credentials of 'more than 10,000 customers' had been 'unlawfully released'.

On 13 October, the country's largest private health insurer, Medibank Private, reported that it was investigating a cyber incident and that 'there is no evidence that any sensitive data, including customer data, has been accessed. [76] For six days, up to 19 October, Medibank was not able to reveal to customers from its own forensic investigation that any data had been stolen, but was forced to confirm its earlier fears that it had been subject to a ransomware attack after a criminal gang contacted it to say that some of the stolen data had been released. The personal health records and personally identifiable data (PID) of more than 10 million existing and former customers had been compromised. The criminals had accessed everything. It was only on 23 February 2023 that the company officially revealed the weaknesses in their cyber security that had allowed the breach to occur. It was breach of the most basic kind.[77]

The reaction reported at the time was one of outrage, largely generated by poor communication strategies and lack of transparency of the two companies.[78] Equally disappointing was the fact that government cyber and law enforcement agencies closed ranks behind the companies and demonstrated little awareness of more effective incident response, let alone a preparedness to admit that the incidents might have reflected that not all was well in the Australian cyber ecosystem.

The Minister for Home Affairs, Clare O'Neil, expressed the view in December 2022 that Australians 'are waking from a cyber slumber'.[79] Her assessment of the previous government's record on cyber security was damning. In parliament, during

discussion of these issues, she hectored the Opposition with taunts of 'you did nothing' in your ten years of government. Officially, she summarised this view as follows:

> We did not do the work nationally over the last decade to help us prepare for this challenge. Prime Minister Morrison's decision to abolish the Cyber Security Ministry when he came to office was a shocker.[80]

O'Neil vowed to 'turn this set of disasters into a permanent step change in cybersecurity for the country' to make it 'the world's most cyber-secure country by 2030'. By the time of the Press Club speech, the new government had taken come measures in response to the data breaches.[81] O'Neil used the occasion to announce another cyber security review to inform the drafting of a new cyber security strategy.

She referenced a seemingly new collaboration between the ASD and the Australian Federal Police involving a 100 person-team permanently assigned to identifying and prosecuting criminal hackers. She acknowledged that 'it will take some time' to see results from this effort. She also announced a specific investigation into lessons learned in the Optus and Medibank attacks.

If O'Neil's assessment was correct, then it can be interpreted as a negative evaluation of what had gone before in national cyber policy. By February 2023, the government announced creation of a new post of Coordinator for Cyber Security to be supported by a National Office for Cyber Security within the Department of Home Affairs.[82] On that occasion, PM Albanese committed to a greater sense of urgency: 'This is a fast-moving, rapidly-evolving threat and for too many years, Australia has been off the pace. Our government is determined to change that'. O'Neill echoed the PM: 'we cannot sleepwalk into our cyber future. I want Australia to be the world's most cyber secure country by 2030. … Government needs to walk the talk'.[83]

Unrevealed Weakness

The urgency of the need for reform was further revealed when the Office of the Australian Information Commissioner (OAIC) reported on 1 March 2023, that there had been a 500% increase (from 1 to 5) on notifiable data breaches in Australia affecting over one million people in the last six months of 2022 compared with the previous six months.[84] The period had seen an increase from 24 to 40 of notifiable data breaches affecting over 5,000 people in the second reporting period.[85] Poor cyber security accounted for a large majority of all breaches reported. One important implication of this release of this data in March is that while domestic debate about data breaches was raging from October through to February, the OAIC had information relevant to the increasing frequency of such attacks that was kept out of the public eye at the time.

MIT Technology Review Insights

In the face of these horror stories and declarations of the need for significant reform, a striking report replaying the country's optimism bias in cyber security evaluations surfaced in the release of the Cyber Defense Index in March 2023 by the MIT Technology Review Insights group. For the top 20 countries, the report assessed 'how well their institutions have adopted technology and digital practices to be resilient against cyberattacks, and how well governments and policy frameworks promote cybersecure digital transactions'.[86] Australia was ranked first in the world for cyber reform, with a summary assessment extracted here in Box 3.

The MIT Technology Review analysis nevertheless is probably flawed. In the first place, making digital infrastructure widely available in no way reflects on how secure it is (though the word 'robust' may be intended to reflect some element of security). Second, the assessment is largely of intentions, not outcomes.

Box 3: CDI Summary Assessment of Australian Cyber Policy

Australia's first-place CDI score reflects efforts to make robust digital infrastructure widely available. The Australian government strives to use digital tools and regulations to safeguard personal data and digital transactions. It committed to overhauling cybersecurity laws, pledging to shelve a previous roadmap. The importance of this was underscored by a hack of Optus, its second-largest mobile carrier, in which 2.8 million records were stolen. Its business leaders have high confidence in the government's cybersecurity stance.

The Index is based mainly on a 2022 survey of around 50 senior executives in each country who

have lead-responsibility for cyber security in their organisation.[87] On the one hand, this is asking essentially for self-evaluation of enterprise cyber security effectiveness by the people charged with undertaking it. On the other hand, it is asking for assessments of the effectiveness of reform of public policy in cyber security by governments from people with little expertise in evaluating public policy reform, except as it affects their enterprise.

In addition to the survey, the report relied in unspecified ways on a diverse range of sources, many of which have their own methodological challenges in terms of reliability.[88] The methodology also included 'primary research interviews with cyber security professionals, technology developers, analysts, and policy makers', 'complemented by a consultative peer-review process with cybersecurity technology analysts'. Relying on these inputs, the authors assigned weighting assumptions 'to determine the relative importance' with which each indicator and pillar influenced a country's cyber security posture'.[89] The 13-person expert panel used by the CDI to review material does not appear to have included anyone with deep expertise in Australian cyber policy.

Minister O'Neil unfortunately claimed that the report 'said Australia's first-place score reflected the Albanese Government's efforts to make robust digital infrastructure widely available'. As can be seen in Box 3, the report did not mention the Albanese government which had only been in government a few months when the analysis had been published.

It is unclear when the survey was conducted or how the framing of the questions might have enabled any distinction between the political agenda of the Albanese government and the robust and wide-ranging reform agenda already in place and being implemented by government officials, business leaders and other stakeholders under the previous government.

Most importantly, the survey and the secondary sources appear to have paid little attention to outcomes in cyber security (increasing numbers of cyber graduates, increasing levels of unprosecuted cyber crime, increasing levels of personal data breaches).

A massive cyberattack on Latitude Financial in Australia, affecting 14 million people , also in March 2023, underscores the ongoing issues and the need for no complacency.[90]

Three Factors for Evaluation

There are three qualitative characteristics of policy reform which might be applied to evaluating the new cyber security strategy:

- a sense of urgency
- a commitment to comprehensiveness and coherence
- investment of political capital for deep reform

Achieving these benchmarks depends on shared leadership by governments, industry, and community actors (especially educators). These elements were not as visible as they needed to be in implementation of the 2016 strategy by national leaders responsible in government, business, and community groups. Much has been achieved in that period and the national scene looks very different in important ways. Yet significant shortcomings remain.

Urgency

The case for urgency is made on a frequent basis, with each new report about the increasing threats and the lack of resolution of underlying shortcomings. On 1 June 2023, the Opposition spokesperson on home affairs and cybersecurity observed that 'that espionage and foreign interference is higher than at any point in our history' and ASD 'has warned of near constant cyber attacks on our government networks and critical infrastructure operators'.[91] On 30 May 2023, the Tech Council reported that the country would have to work harder to deliver the 'hundreds of thousands more people working in tech to meet the country's expected digital needs over the next decade'.[92]

The US adopts a far greater sense of urgency than Australia. On 29 March 2023, US President Joe Biden renewed the national state of emergency in cyberspace first declared by President Obama on 1 April 2015 and renewed every year since then.[93] The Admin-istration noted that 'significant malicious cyber-enabled activities continue to pose an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States'.

By 2022, Australia began to approach the attitude of urgency adopted by the US seven years earlier. In issuing a new 'Australian Government Crisis Management Framework' in November of that year, the federal government had more fully incorporated cyber emergencies into national policy.[94] Australia does not however appear to have realised the potential value of declaring a national emergency in cyberspace. As the Royal Commission into Natural Disaster Arrangements observed, the value of such a declaration in those circumstances can be substantial: 'A declaration would signal to communities the severity of a disaster early, act as a marshalling call for the early provision of Australian Government assistance when requested, facilitate coordination with state and territory emergency management frameworks, and, in very limited circumstances, allow the Australian Government to act without a request from a state or territory'.[95]

The current emergency response framework does not specifically list a 'cyber' emergency among the items on a list of ministerial responsibility, but it would be covered under the provision that the Minister for Home Affairs is responsible for 'Domestic security-related incidents (excluding terrorist incidents) or other domestic crises with no clear ministerial lead'.[96] It does say elsewhere that the relevant policy governing response coordination will be in line with the 'Cyber Incident Management Arrangements'.[97] ASD would be the lead agency coordinating the response. The federal government reports only low to moderate take-up by government agencies of important ASD-recommended preparedness measures.[98]

While the administrative significance of declaring a national emergency in cyberspace differs quite substantially for Australia compared with the US, the Australian government might benefit from a shift in its rhetoric to be more consistent about the urgency of the threat. Reporting processes in the federal government for cyber attacks on Australia and alert notices for possible cyber vulnerabilities (at the technical level) have improved substantially in recent years, but the quality of the data provided by government leaves much to be desired.

There has been little transparency from the companies affected by mass breaches of personal information in 2022 and 2023 (Optus, Medibank, and Latitude) about why their systems failed to prevent the attacks and then failed to adequately compartmentalise the sensitive personal information.

Moreover, reporting on cybercrime (especially prosecutions and convictions) remains woeful at federal and state level. The lack of qualitative, regular and in-depth reporting on cyber crime in Australia undermines the efforts of governments to mobilise more effective defences. The lack of success by Australian police forces, especially the Australian Federal Police, in bringing cyber criminals to justice, or at least ending their attacks, is also an indicator of lack of urgency by Australian governments. It can be seen as an issue of priorities (catching cyber criminals versus the prevention of domestic violence) but the balance does not appear to go far enough in the direction of support for cyber security policing. Governments need urgent solutions in both areas of criminality, so obviously need to spend a lot more in both areas and focus the spending more effectively.

Another important indicator of urgency might be a commitment by governments to reach certain targets in addressing the cyber skills gap, then perhaps the government could commit to closing that gap completely. For example, if the current skills deficit for 2025 is assessed at 3,000, can the federal and state governments commit to closing that gap by 2025? At present, the main benchmarks appear to be merely an improvement in the size of the available work force rather than a commitment to securing enough skilled professionals, either through education of Australians or through skilled migration programs. In fact, the skills deficit is not as simple as that, but the absence of any targets for closing the gap seems to undermine the credibility of government claims of urgent threat. The commitments by ASD and Defence in 2020 to expand their work force by a large figure, and then in 2022 under Project Redspice to increase that figure for 'analyst, technologist, corporate and enabling roles' to 1900[99] was a strong indicator of greater urgency, but that ambition was not ever mapped out in public with a credible cyber security education strategy for Australian citizens (that is people who can receive a security clearance for working with the most sensitive intelligences sources and methods).

A new body, Jobs and Skills Australia, was legislated on 16 November 2022, and this legislation was amended on 23 March 2023 to finalise its structure as a tripartite, statutory body designed to guide response to Australia's workforce challenges. It has

yet to zero in on cyber-skills as a defined priority for its work. Likewise, the relevance of the Government response for the March 2023 Parkinson Report on Immigration[100] needs incorporation here, as will the forthcoming report of the Universities Accord Panel.

There would need to be a clearer sense of urgency in legal reform for cyber policy in Australia. It has largely been reactive, and it typically defaults to more power for the governments and less power for citizens. The country's laws do not compare favorably to those in leading peer jurisdictions in comprehensiveness, reach and effectiveness. The artificial intelligence revolution is already occurring, and Australian law reform is not moving quickly enough for the challenges that this brings to cyber security policy and operations.

Coherence

According to the OECD, policy coherence is not only economically valuable but essential for achieving primary goals. The first requirement for coherence if applied to the field of cyber security is that a policy (or set of policies) should address all the key planks or pillars – that it should be comprehensive and address:

- low rate of arrests and convictions for cyber crime
- special protections for children and other vulnerable groups
- security of personal information/data
- security of systems
- formal and informal digital education
- community awareness
- privacy protection
- national digital transformation
- advancing national security and defence.

A view of the types of policies needed to achieve policy coherence is in Box 1 above.

Policy coherence can be demonstrated by identification of clear synergies between specific programmatic activity undertaken under separate pillars and across the full relevant system producing the results to be addressed. A mere claim of synergy, for example, between more cyber security education and improved workforce outcomes, would be inadequate.

A mature test of coherence might involve the identification of clear trade-offs between spending on programmatic activity undertaken under separate pillars. For example, a policy might usefully say we have made a conscious decision to spend only small amounts on capturing cyber criminals since this would be less productive than using the available investment funds for community education about the threats and resilience. This point is debatable but coherence can only de demonstrated by discussing and analysing the relationship between pillars of policy.

Cyber coherence is also more likely to be in play when the government is focused on creating a cyber ecosystem rather than simply addressing independent pillars of activity. Cyber security education must be addressed as an ecosystem issue, not as segmented. Increasing cyber crime could be seen as a failure of the policies for a cyber education ecosystem in business and communities.

Most importantly, policy coherence should be measured and documented. For this, longitudinal studies and comprehensive evidence collection against evaluation criteria would be essential components. For this reason, university-based researchers expert in public policy would be essential actors since only they can provide the necessary rigor and expertise for sustained longitudinal analysis. Most governments around the world have not performed well in this area, and the Australian government has also shown itself unable to do it.

Depth

We need to set targets that represent deep transformation, not simply marginal increases on performance. For example, instead of lazy targets such as a ten percent increase over five years in cyber graduates from university programs, we should have specialisation-specific outputs that can trigger radical outcomes, such as 50% growth in graduate numbers in threat intelligence. But for that we may need first a university program in cyber threat intelligence, with the spending programs from government and industry to match.

We would want to see evaluation of targets against the depth criterion.

We would want to see higher visibility for the inclusion of specialists in setting targets and monitoring them, not just broad consultation when a new strategy is being considered. True specialisation would be manifested in university-sector review of any reports by consulting companies such as the Big Four, as made even more clear by the public controversy about the activities and conflicts of interest for PwC that emerged in May 2023. Thus depth would depend on a comprehensive set of bodies and nodes of action that frequently contribute to cyber policy deliberation, planning and evaluation.

Another aspect of depth in policy reform would be an expansion of the number and types of actors involved in behavioural change and stronger networking of them into a force for change. In this respect, creating umbrella organisations or nodes is certainly useful. For example, as part of its 2016 package reforms, the Turnbull government began to set up cyber security nodes in the capital cities to bring together key actors. This was a step toward greater depth in reform policies but the initiative is still maturing. One test of their reach in 2023 and beyond would be to review the activities of the nodes outside the state capitals. A second type of deepening mechanism would be the creation of a cyber militia, or a 'neighbourhood watch' for cyberspace, where vulnerable users or simply serious users can gather for cyber security refinorcement. Another vehicle would be to rely on existing groups (professional associations, local councils, industry associations, community welfare groups) to be a focal point of new activity.

The best single test of a government's commitment to depth would be its new spending on cyber security education, including moves to make security in cyberspace a compulsory subject of education at all levels. Some have made the comparisons with road safety messaging and education, but in fact serious cyber security education would need to incorporate aspects of sex education, mental health education and basic education about forms of online crime.

Compiling the Evidence Base

When left to their own devices to evaluate their cyber programs, governments around the world generally settle for a process of cherry-picking available activity data to demonstrate policy success, regardless of many shortcomings. Governments often avoid setting concrete targets lest they be forced to report shortfalls. Australian cyber policy practice on evaluation has been exactly that: cherry-picking to claim positive outcomes and little attention to assessments that may be negative. As noted above, the ANAO called this 'optimism bias'.

In Australia, one creditable exception to the 'selective evidence' approach in other fields of public policy has been the setting of comprehensive benchmarks and targets for outcomes in 'closing the gap' in standards of living and social outcomes for the country's indigenous people. This self-executing evaluation process has been accompanied by a legal obligation to report each year to the government and the national parliament. One example of a desired outcome of the strategy among 19 socio-economic goals is that 'Aboriginal and Torres Strait Islander people enjoy long and healthy lives' and the quantitative target is that the gap in life expectancy between those communities and the rest of Australia will be eliminated by 2031.[101] The 'targets are specific and measurable goals that will be monitored to show how progress is being made across each of the outcome areas. Under each of the targets there are indicators that help to provide an understanding of how progress will be tracked'.[102]

The political authority is a Joint Council representing a unique partnership between 'the Commonwealth Government, state and territory governments, the Coalition of Aboriginal and Torres Strait Islander Peak Organisations (the Coalition of Peaks) and the Australian Local Government Association'. The reporting authority is the country's Productivity Commission, but it relies on data collected largely by other credible and authoritative organisations, including members of the Joint Council, and it maintains a publicly available and consistent database available for public scrutiny.

Data to assess the progress of policy goals is not created by the authors of the evaluation (the annual 'Closing the Gap' report). It is collected and assessed with input from the Australian Bureau of Statistics (BAS) and the Australian Institute of Health and Welfare (AIHW). The current national agreement on 'Closing the Gap' includes a new data development plan.[103] This stipulates that the plan will 'outline clear timeframes for actions to be delivered and which Party will be responsible for each action'.

Cyber Data Development Plan

Emulating the approach used for 'Closing the Gap' in indigenous policy, an evaluation methodology for national cyber policy reform must include a data development plan. There has been some progress on this in the Department of Home Affairs but the data collection is not closely enough tied to criteria for assessing outcomes. The Productivity Commission might be the most suitable agency for leading the development of such a data development plan, but the process would need to involve multiple stakeholders, all of whom are committed to bringing about the declared national goals in cyber security and all of whom have capabilities in the related data development for public consumption.

The Annual Threat Report of the Australian Cyber Security Centre (ACSC) might be one place where the Australian government could canvas improvements resulting from cyber policy. According to the 2020-21 version there appears to have been a considerable increase in investment and much policy innovation, but with little improvement in national cyber security performance and large-scale increase in threat (such as a 75% increase in cyber intrusions related to ransomware).[104] This correlation between increased investment in cyber security (billions of dollars) and little appreciable increase in security is one reason why many private sector firms are stalling in their investments and many workers are taking cyber security less seriously. The lack of credible evaluation of performance, accompanied by appropriate metrics, weakens the possibility of greater cyber policy improvement.

Conclusion: Towards Urgency, Coherence, and Depth

The discussion leads us to the following questions:

- Who should evaluate Australian cyber policy and how often?
- What benchmarks should be used for evaluation?
- What would be a practicable balance between qualitative and quantitative evaluation?
- What would be a practicable balance between evaluating inputs, outputs, and outcomes?
- What would be involved in creating a federated ecosystem for cyber policy evaluation in Australia?

Basic Principles

1. The federal government should align its evaluation processes with the appropriate strategic focal points, especially the prevention of cyber harms to the country, its businesses, and its citizens. There should be a single overall evaluation (to ensure coherence between policy pillars) as well as separate evaluations of each key policy pillar.
2. The evaluations must be independent and therefore led by an eminent social scientist, expert in policy evaluation and policy reform, who as 'evaluation leader' reports to the Department of Prime Minister and Cabinet.
3. The mechanism of evaluation should include several distinct panels specialising in sub-elements of national cyber policy (countering cybercrime, protection of citizens' rights, technical aspects of cyber security, education, and workforce development).
4. The evaluation criteria and terms of reference can be set once the mechanisms of evaluation are in place since the criteria and performance indicators would need to be determined by the expert panels under the guidance of the evaluation leader.
5. The evaluations must be highly transparent and open to public scrutiny (subject to the content detail not offering sensitive information to cyber-criminals or hostile governments).
6. The overall policy should be evaluated by this independent process every four years, with all sub-components evaluated at least every two years, bearing in mind that the Department of Finance has advised that evaluation should be a continuing and permanent element of policy delivery and there is a new Australian Centre for Evaluation being established in Treasury to operate from 1 July 2023.
7. The government must commit to the best standards of evaluation and not limit itself to those currently practised by the Department of Home Affairs in its annual reporting on

cyber security performance. This paper assesses those to be less rigorous than those conducted even currently by other government departments, such as the Department of Industry.

8. Given the importance of cyber security to national security, the federal government should commit at least 3% of all cyber security component spending to evaluation of their execution and outcomes.

Strategic Focus on Cyber Harms

Australia's cyber security policy must be assessed against its reduction of cyber harms, the mitigation of cyber harms, and the prevention of cyber harms.

These harms, by source, include:

- Hostile state activity.
- Criminal activity in cyberspace.
- Anti-social but lawful practices.
- Incompetence by users or operators.
- Unforeseeable effects created by coincidence of negative events.

To address cyber harms from these sources is the most urgent purpose of cyber security policy. The prioritization in evaluation of urgent purposes over non-urgent purposes is an essential departure point.

Non-urgent purposes, though very important, would be those designed to create social or economic value for its own welfare gains and have less to do with protection in cyberspace. Such welfare gains include:

- Improved ICT knowledge and skills
- Improved economic gains
- More creative uses of cyberspace.

Strategic Focus on Outcomes: Reduction in Cyber Harms

The evaluation of cyber security policy must have a laser-like focus on outcomes: a measurable reduction in cyber harms and a measurable growth in national confidence that cyberspace is more secure and productive and less threatening as a result of national cyber policy.

Strategic Focus on Whole of Society

The evaluation must be rooted in the reality that improved cyber security outcomes in Australia need to be delivered by many actors working in close coordination, and the outcomes shaped by these actors should be focal points of evaluation:

- National security agencies and their international partners capable of preventing or mitigating cyber harms.
- Domestic police forces and their international partners capable of successful prosecutions for cybercrime and related prevention activities.
- National, state-based, local and international actors whose mission is mitigation of the most serious cyber effects.
- A vibrant and responsive system of laws and regulations.
- A highly developed research ecosystem focused on national cyber security outcomes.
- Domestic and international news media that act responsibly and are well-informed.
- Civil society actors, in Australia and internationally, mobilised around the goal of improved protection in cyber space.

The federal government should consider bringing national cyber security out from under the shadows of the Australian Signals Directorate (ASD) even more than it has since 2016. This would allow it to concentrate much more on espionage and military issues while giving a more robust and fully independent role to the National Cyber Security Centre as a non-defence agency, modelled on the US Cybersecurity and Infrastructure Security Agency (CISA).

Strategic Focus on Rights and Obligations

An overarching approach to evaluation must include assessment of impacts on citizens' rights and obligations. In particular, there needs to be much more attention paid to privacy issues arising from breaches of sensitive personal data.

Individual Program Evaluations

The framework should allow for individual program evaluations, of which the federal government's formal 'Cyber Security Strategy' is but one program, and not the totality of national effort in cyber security policy that needs to be evaluated.

The current government has identified core policy areas for the forthcoming strategy, but these cannot be allowed to dominate the evaluation because that

would seriously degrade the strategic focus described on the preceding page. These are necessary, but far from sufficient. These core policy areas identified by the government are:

- A secure economy and thriving cyber ecosystem.
- A secure and resilient critical infrastructure and government sector.
- A sovereign and assured capability to counter cyber threats.
- Australia as a trusted and influential global cyber leader, working in partnership with our neighbours to lift cyber security and build a cyber resilient region.[105]

The way the government organises its cyber security strategy around these four themes blurs fundamental priorities, such as security and business growth, that deserve much sharper articulation separately. These four policy themes appear to overlook others which have very high priority (such as reducing cybercrime). Australia's policies for countering and mitigating cybercrime are one of its weakest areas. The latest ACSC Threat Report records an annual 76,000 cybercrime reports, an increase of nearly 13 per cent from the previous financial year.[106]

---

[1] The Australian Federal Government released cyber security strategies in 2009, 2016 and 2020.
[2] Australian Government, 2023 - 2030 Australian Cyber Security Strategy Discussion Paper', 2023, p. 25, https://www.homeaffairs.gov.au/reports-and-pubs/files/2023-2030_australian_cyber_security_strategy_discussion_paper.pdf.
[3] Greg Austin, 'Australia's digital skills for peace and war', *Journal of Telecommunications and the Digital Economy,* 2.4 (2014) 68-1; Greg Austin, 'Australia Rearmed!: Future Needs for Cyber-enabled Warfare', Australian Centre for Cyber Security, 2016, Australian Centre for Cyber Security, UNSW Canberra, Working Paper #1, available at https://www.socialcyber.co/_files/ugd/15144d_6a1eb662e90e4c96beb5ccfa655cbc6a.pdf?index=true; Greg Austin and Jill Slay. 'Benchmarking Australia's Cyber Security Strategy: A Future-Looking Checklist', UNSW Australian Cyber Security Centre, UNSW Canberra, Briefing Paper#1, 2016, available at https://www.socialcyber.co/_files/ugd/15144d_af098d83a1b74f818872f51cb6eeeb2d.pdf?index=true; Greg Austin 'Human Capital for Cyber Security: The Australian Case', Australian Centre for Cyber Security, Canberra, ACCS Discussion Paper #2, November 2017; Greg Austin, 'Are Australia's responses to cyber security adequate?', in *Australia's Place in the World 2017*, Report by the Committee for the Economic Development of Australia, 50-61; and Greg Austin and Gary Waters, 'Australia Needs Civil Defence against the Cyber Storm', Research Group Cyber War on and Peace, UNSW Canberra Cyber, March 2019.
[4] Greg Austin, *Cyber Policy in China*, Polity, 2014; Greg Austin, *Cybersecurity in China*, Springer, 2018; and Greg Austin and Wenze Lu, 'Five Years of Cyber Security Education Reform in China', in Greg Austin (ed), *Cyber Security Education: Principles and Policies*, Routledge, 2020, 173-193.
[5] See IISS, *Cyber Capabilities and National Power: A Net Assessment*, London 2021, https://www.iiss.org/blogs/research-paper/2021/06/cyber-capabilities-national-power.
[6] Greg Austin ed., *Cyber Security Education: Principles and Policies*, Routledge 2020.
[7] Greg Austin ed., *National Cyber Emergencies: The Return of Civil Defence*, Routledge 2020.
[8] Department for International Development, 'Evaluation of the Conflict Prevention Pools Synthesis Report', 2004, 83pp plus annexes, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/67935/ev647synthesis.pdf. The synthesis report was based on six separate case study reports, and a Portfolio Review.
[9] See for example Austin and Slay. 'Benchmarking Australia's Cyber Security Strategy'.
[10] Sigurdur Helgason, 'International Benchmarking: Experiences from OECD Countries', Paper Presented at a Conference Organised by the Danish Ministry of Finance on International Benchmarking, Copenhagen, 20-21 February 1997, p. 2, www.oecd.org/governance/budgeting/1902957.pdf.
[11] HMG, 'The Green Book', 2022, p. 2, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1063330/Green_Book_2022.pdf.
[12] Ibid.
[13] Matthew Gray and J. Rob Bray, 'Appendix B: Evaluation in the Australian Public Service: current state of play, some issues and future directions. An ANZSOG research paper for the Australian Public Service Review Panel', March 2019, pp. 11-12, https://www.apsreview.gov.au/sites/default/files/resources/appendix-b-evaluation-aps.pdf.
[14] Ibid. p. 13.
[15] Ibid. p. 7.
[16] See Tom Burton, 'This $10m idea aims to save taxpayers $200m in consulting fees', Australian Financial Review, 27 April 2023, https://www.afr.com/politics/federal/this-10m-idea-aims-to-save-taxpayers-200m-in-consulting-fees-20230427-p5d3ny. According to Burton, 'A new Treasury evaluation unit, costing $10 million over the next four years, is expected to recoup up to $200 million in consultant savings, as the federal government targets waste and ineffective programs. The new unit, an election pledge, will work with other federal agencies to more consistently evaluate key programs, rebuild lost internal evaluation capability, and support high-quality evaluation such as better data practices.'
[17] Department of Industry, Innovation and Science, 'Evaluation Strategy 2017-2021', 2017, https://www.industry.gov.au/sites/default/files/2022-09/67013_-_combined_document.pdf. This document was only made public after a request under the Freedom of Information Act.
[18] See Department of Industry, Science, Energy and Resources, 'Cooperative Research Centres Program Impact Evaluation. 30 November 2021, https://www.industry.gov.au/sites/default/files/2023-01/cooperative-research-centres-program-impact-evaluation.pdf. Of

note, the CRC evaluation found that there had been no alignment between cyber CRC project grant completions and the government's manufacturing priorities (p. 74), while in other CRCs there had been many. The evaluation also found that one cyber CRC project would provide forward benefits worth $62.7 million (p. B-9).It also claimed $134.5 million benefit into the future by 'reduce[d] costs for government, the community and industry through robust advice, awareness raising and examination of outcomes for complex problems' (B-10).

[19] Department of Industry, Science, Innovation and Resources, 'Industry Growth Centres Initiative Initial Impact Evaluation', 2022, p. 19, https://www.industry.gov.au/sites/default/files/2022-11/industry-growth-centres-initiative-initial-impact-evaluation.pdf. AustCyber had received $40 million over six years (FY2017 to FY2021)(p. 40).

[20] Gov.uk, 'Evaluation Strategies from UK Government Departments', undated, https://www.gov.uk/government/collections/evaluation-strategies-from-uk-government-departments.

[21] See Department of Homeland Security, 'Evidence and Evaluation Plans', undated, https://www.dhs.gov/evaluation-and-evidence-plans.

[22] See Department of Finance, 'Evaluation in the Commonwealth (RMG 130)', updated 21 December 2022, accessed 13 April 2022, https://www.finance.gov.au/government/managing-commonwealth-resources/planning-and-reporting/commonwealth-performance-framework/evaluation-commonwealth-rmg-130.

[23] Ibid. The guidance 'does not create any new mandatory requirements in relation to evaluation – those responsible for the successful delivery of results need to determine fit for purpose evaluative approaches for specific government programs and activities in a particular context.'

[24] Department of Home Affairs, '2021-22 Annual Report', 2022, accessed through Australian Government Transparency Portal, 13 April 2022, https://www.transparency.gov.au/annual-reports/department-home-affairs/reporting-year/2021-22-10.

[25] Ibid.

[26] See Clare O'Neil, 'Home Affairs and the long view -National Press Club Address', 8 December 2022, https://minister.homeaffairs.gov.au/ClareONeil/Pages/national-press-club-address.aspx.

[27] Greg Austin and Jill Slay, 'Australia's Response to Advanced Technology Threats: An Agenda for the Next Government', UNSW Canberra, Canberra, Australian Centre for Cyber Security Discussion Paper 3 (2016), p. 5, available at https://www.social-cyber.co/_files/ugd/15144d_9e5656980b764585ae5f6032f8de83bc.pdf?index=true.

[28] The Australian Cyber Security Centre (ACSC) within the Australian Signals Directorate (ASD) 'leads the Australian Government's efforts on national cyber security. It brings together cyber security capabilities from across the Australian Government to improve the cyber resilience of the Australian community and help make Australia the most secure place to connect online.' See ASD, 'Cyber Security', https://www.asd.gov.au/cyber-security.

[29] Australian Government, 'Australia's Cyber Security Strategy 2020, p. 16, https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf.

[30] Simonetta Astolfi and Claire Grundy, 'Disclosure of confidential information by Commonwealth officers – repeal of section 70 of the Crimes Act 1914 (Cth)', Maddocks, Legal Insights, 23 July 2019, https://www.maddocks.com.au/insights/disclosure-of-confidential-information-by-commonwealth-officers-repeal-of-section-70-of-the-crimes-act-1914-cth#:~:text=For%20more%20than%2050%20years,and%20former%20'Commonwealth%20officers'.

[31] There are numerous sources who make this comment. See for example, Paul Gregoire, 'Federal Freedom of Information Laws Enhance Government Secrecy', 23 July 2021, https://www.sydneycriminallawyers.com.au/blog/federal-freedom-of-information-laws-enhance-government-secrecy/.

[32] See David Watts and Pompeu Casanovas, 'Privacy and Data Protection in Australia: A Critical Overview (extended abstract)', 27 June 2019, https://www.w3.org/2018/vocabws/papers/watts-casanovas.pdf. The authors note (p.3) that 'at a Commonwealth level, Australia's information privacy laws have lagged behind European developments and the introduction of new technologies that challenge existing forms of protection.'

[33] Elizabeth Byrne, 'With the sentencing of Witness J now public, the federal government is exploring how it can avoid anything like it happening again', ABC News, 20 April 2023, https://www.abc.net.au/news/2023-04-20/the-unusual-and-secret-case-of-witness-j/102244966.

[34] Damien Cave, 'Australia May Well Be the World's Most Secretive Democracy', New York Times, 5 June 2019, https://www.nytimes.com/2019/06/05/world/australia/journalist-raids.html.

[35] See Parliamentary Joint Committee on Intelligence and Security, 'C. Timeline of Reviews', undated, https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/IntegrityMeasuresBill/Report/section?id=committees%2Freportjnt%2F024737%2F78649. The reviews have included: two separate inquires led by Justice Hope in 1974 and 1983; the Flood Review in 2014; the Independent Review of the Intelligence Community in 2011; the Independent Intelligence Review (IIR) in 2017; and the Comprehensive Review of the Legal Framework of the National Intelligence Community (Richardson Review) in 2019.

[36] See DFAT, '2022 Annual Development Evaluation Plan', 2022, https://www.dfat.gov.au/sites/default/files/annual-development-evaluation-plan-2022.pdf.

[37] Austin, 'Australia Rearmed!: Future Needs for Cyber-enabled Warfare', p. 2.

[38] Austin and Slay, 'Benchmarking Australia's Cyber Security Strategy'.

[39] Department of Prime Minister and Cabinet, 'Australia's Cyber Security Strategy', 2016, p. 57, https://www.homeaffairs.gov.au/cyber-security-subsite/files/PMC-Cyber-Strategy.pdf.

[40] Greg Austin and Jill Slay. 'Australia's Response to Advanced Technology Threats: An Agenda for the Next Government', UNSW Canberra, Canberra, Australian Centre for Cyber Security Discussion Paper 3 (2016), p. 5.

[41] Zoe Hawkins and Liam Nevill, '2016 Cyber Security Strategy: the perils of self-assessment', The Strategist, 27 April 2017, https://www.aspistrategist.org.au/2016-cyber-security-strategy-perils-self-assessment/.

[42] IISS, Cyber Capabilities and National Power: A Net Assessment', p. 48.

[43] Australian Cyber Security Growth Centre, 'Australian Cyber Security Sector Competitiveness Plan', 2017, https://www.austcyber.com/file-download/download/public/327.

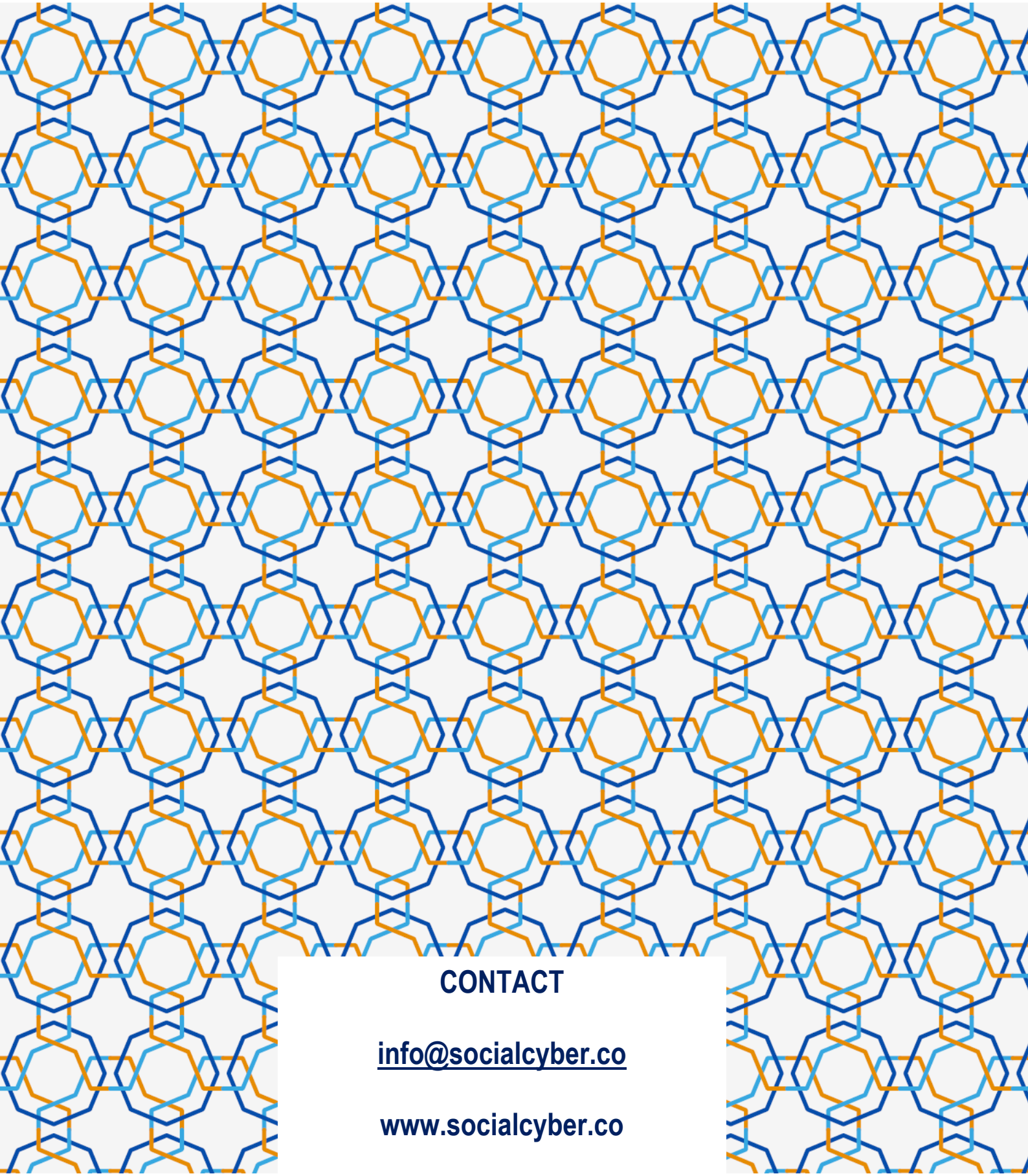
[44] Ibid., p. 2. Note that the pagination in this report carries duplicate page numbers.
[45] AustCyber, 'Australia's Cyber Security Sector Competitiveness Plan 2020 Update: Driving growth and global competitiveness', 2020, https://www.austcyber.com/file-download/download/public/1170.
[46] The ANAO summarised its review practice in the field of cyber security beginning in 2014. 'The ANAO has contributed to an improved awareness of cyber security risks and key mitigating controls across Government since 2014, although [it] has only reviewed eleven different Australian Government entities over this period. In April 2013, AGD [the Attorney General's Department] made amendments to the PSPF mandating the Top Four [cyber mitigation strategies] to be enacted with immediate effect. As a result, in 2014, the ANAO undertook a review of seven Australian Government entities to assess their compliance with the Top Four.' … … As part of the 2016/17 AAWP, the ANAO conducted 1 out of a total of 57 performance audits with a cyber security focus. This audit was a follow up review on a previous ANAO cyber security related performance audit, and as a result, the scope included only 3 out of more than 200 Australian Government entities'. See Australian National Audit Office, 'Review of Cybersecurity', 2017, p. 8, https://www.anao.gov.au/sites/default/files/ANAO-Review_of_Cyber_Security.pdf.
[47] Ibid., p. 7.
[48] Ibid., p. 10.
[49] See Michael Slezak and Ariel Bogle, 'Australian government departments are routinely audited for cyber readiness. Most fail', ABC News, 20 June 2020, https://www.abc.net.au/news/2020-06-20/australian-departments-routinely-audited-for-cyber-readiness/12375050.
[50] 'In line with the requirements of the Information Security Manual, including the Top Four and other mitigation strategies in the Essential Eight.' See ANAO, 'Cyber Resilience of Government Business Enterprises and Corporate Commonwealth Entities', 2019, online version, https://www.anao.gov.au/work/performance-audit/cyber-resilience-government-business-enterprises-and-corporate-commonwealth-entities.
[51] Joint Committee on Public Audit and Accounts, 'Report 485 Cyber Resilience', December 2020, https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Public_Accounts_and_Audit/CyberResilience2019-20/Report. This assessment is carried in IISS, 'Cyber Capabilities and National Power', p. 51.
[52] In the case of Defence, see ANAO, 'Delivery of Security Vetting Services Follow-up', December 2020, https://www.anao.gov.au/work/performance-audit/delivery-security-vetting-services-follow-up.
[53] ANAO, 'Auditor-General's mid-term report', 2020, https://www.anao.gov.au/work/speeches-and-papers/auditor-generals-mid-term-report.
[54] Department of Defence, '2020 Defence Strategic Update', 2020, p. 27, https://www.defence.gov.au/sites/default/files/2020-11/2020_Defence_Strategic_Update.pdf.
[55] Australian Government, Department of Home Affairs, 'Australia's Cyber Security Strategy', Canberra, August 2020, https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf.
[56] IISS, 'Cyber Capabilities and National Power', p. 48.
[57] Australian Government, 'Australia's Cyber Security Strategy2020', 2020, pp. 44-46, https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf.
[58] 'Australia's Cyber Security Strategy2020', p. 44.
[59] 'Cyber Security Industry Advisory Committee Annual Report 2021', 2021, pp. 25-37, https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020-annual-report-2021.pdf.
[60] Ibid., p. 6.
[61] 'Cyber Security Industry Advisory Committee Annual Report 2022', 2022, p. 10, https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-IAC-annual-report-2022.pdf.
[62] Ibid.
[63] 'Cyber Security Industry Advisory Committee Annual Report 2022', 2022, p. 9, https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-IAC-annual-report-2022.pdf.
[64] Ibid., p. 18
[65] Ibid., pp. 24-6.
[66] Ibid., pp. 24-5. The aim was to 'ensure policy makers delivery informed and evidence-based solutions for future skills demands'. The projects included 'working with:

- the Australian Bureau of Statistics (ABS) to update the Australian and New Zealand Standard Classification of Occupations (ANZSCO) to better reflect cyber security and related occupations
- the Behavioural Economics Team of the Australian Government to research people's decisions in relation to working in cyber security
- the Australian Strategic Policy Institute to research the cyber security sector products, technologies, skills and capabilities needed to protect Australia's national interests.

At the date of publication of this report, the author has been unable to find publicly available information on the current state of progress in this work.
[67] 'Cyber Security Industry Advisory Committee Annual Report 2022', p. 24.
[68] Ibid., p. 26.
[69] ANAO, 'Administration of Critical Infrastructure Protection Policy', 2022, online version, https://www.anao.gov.au/work/performance-audit/administration-critical-infrastructure-protection-policy.
[70] ANAO, 'ANAO Annual report 2021-22, 2022, https://www.anao.gov.au/work/annual-report/anao-annual-report-2021-22. The report said: 'While the ANAO's performance and financial audits point to many areas of high quality and effectiveness within the public sector, there continues to be evidence that the sector's approach to some core activities regularly falls short of expectations. This is especially prevalent in the areas of cybersecurity, procurement, and grants administration'.
[71] ANAO, 'Management of Cyber Security Supply Chain Risks', December 2022, online version, https://www.anao.gov.au/work/performance-audit/management-cyber-security-supply-chain-risks.

[72] AustCyber, 'Australia's Cyber Security Sector Competitiveness Plan 2022', Executive Summary, November 2022, online version, https://www.austcyber.com/resources/scp-2022/executive-summary.
[73] Ibid., Chapter Two, https://www.austcyber.com/resources/scp-2022/chapter-2.
[74] Optus, 'Optus notifies customers of cyberattack compromising customer information', 22 September 2022, https://www.optus.com.au/about/media-centre/media-releases/2022/09/optus-notifies-customers-of-cyberattack.
[75] For a chronology of announcements by Optus, see Optus, 'Latest updates & support on our cyber response', undated, https://www.optus.com.au/support/cyberresponse, accessed 8 March 2023.
[76] Medibank Private, 'Cyber Event Timeline', undated, https://www.medibank.com.au/health-insurance/info/cyber-security/timeline/, accessed 8 March 2023.
[77] Ibid. 'The criminal accessed our systems using a stolen Medibank username and password used by a third-party IT service provider; The criminal used the stolen credentials to access Medibank's network through a misconfigured firewall which did not require an additional digital security certificate; the criminal was able to obtain further usernames and passwords to gain access to a number of Medibank's systems and their access was not contained.'
[78] 'The lack of transparency [from Medibank] has been appalling. Their lack of openness to the Australian public on what went wrong and what they're going to do to fix it is non-existent. There's been nothing, and their lack of engagement with their outraged customers is palpable. Apart from the fact that they were hacked, they've said nothing about what protection measures they had in place to make sure that hackers couldn't get access to all these records. They've said nothing about what they're going to do internally in terms of new investments in cybersecurity. They've said zero. The question we don't know is, how much was Medibank paying for cybersecurity? How big was the cybersecurity department? Was it expanding? Was it shrinking? A company like Medibank has the assets to prevent the loss of this data through simple, disciplined security measures, and they apparently didn't take them. Medibank needs to explain itself.' See Claudia Glover, 'Medibank criticised for 'appalling' lack of transparency as stolen data leaks online', TechMonitor, 14 November 2022, https://techmonitor.ai/technology/cybersecurity/medibank-cybersecurity-hack-australia.
[79] See Clare O'Neil, 'Home Affairs and the long view -National Press Club Address', 8 December 2022, https://minister.homeaffairs.gov.au/ClareONeil/Pages/national-press-club-address.aspx.
[80] Ibid.
[81] Ibid. It had legislated a new set of penalties regime under existing Privacy Law to encourage business to do better at cyber security. It also announced a new contribution of effort to the 36-country Counter-Ransomware Initiative.
[82] Minister for Home Affairs, 'Prime Minister's Cyber Security Roundtable: Joint media release with the Hon Anthony Albanese MP', 27 February 2023, https://minister.homeaffairs.gov.au/ClareONeil/Pages/prime-minister-cyber-security-roundtable.aspx.
[83] Ibid.
[84] Office of the Information Commissioner, 'Notifiable data breaches report July to December 2022', 2023, p. 10, https://www.oaic.gov.au/__data/assets/pdf_file/0026/39068/OAIC-Notifiable-data-breaches-report-July-December-2022.pdf.
[85] Ibid.
[86] MIT Technology Review Insights, Cyber Defense Index 2022/23', 2023, p. 4, https://www.technologyreview.com/2022/11/15/1063189/the-cyber-defense-index-2022-23/.
[87] Ibid. 'Respondents rated the effectiveness of technology adoption, policy, and regulation formation, and their own cybersecurity activities, as well as their technology development priorities over the next two to three years. The survey response data was converted into scores, where each country's responses were ranked according to their variance from the mean of the global average.'
[88] The included the UN E-Government Knowledgebase, Data Center Map, Worldometer, Global Change Data Lab, Global Cybersecurity Index (GCI) of the International Telecommunication Union (ITU), the UN Conference on Trade and Development (UNCTAD), the World Bank Group, and Oxford Insights.
[89] MIT Technology Review CDI, 'About', https://www.technologyreview.com/2022/11/15/1063189/the-cyber-defense-index-2022-23/ accessed 8 March 2023.
[90] Ry Crozier, 'Latitude Financial Counts the Cost of Cyber Attack', IT News, 26 May 2023, https://www.itnews.com.au/news/latitude-financial-counts-the-cost-of-cyber-attack-596270.
[91] James Patterson, 'Speech to the Australian Cyber Security Connect Summit', I June 2023, https://www.senatorpaterson.com.au/news/speech-to-the-australian-cyber-security-connect-summit.
[92] Tech Council, 'Australia Set To Deliver 1.2 Million Critical Tech Workers By 2030 To Drive Productivity Across The Australian Economy', 30 May 2023, https://techcouncil.com.au/newsroom/australia-set-to-deliver-1-2-million-critical-tech-workers-by-2030-to-drive-productivity-across-the-australian-economy/.
[93] White House, 'Notice on the Continuation of the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities', 29 March 2023, https://www.whitehouse.gov/briefing-room/presidential-actions/2023/03/29/notice-on-the-continuation-of-the-national-emergency-with-respect-to-significant-malicious-cyber-enabled-activities-3/.
[94] Australian Government, 'Australian Government Crisis Management Framework', November 2022, https://www.pmc.gov.au/sites/default/files/resource/download/australian-government-crisis-management-framework.docx.
[95] Royal Commission into National Natural Disaster Arrangements, 'Report', 2020, https://naturaldisaster.royalcommission.gov.au/publications/html-report/chapter-05.
[96] 'Australian Government Crisis Management Framework', p. 16.
[97] Ibid., p. 44.
[98] ACSC, 'The Commonwealth Cyber Security Posture in 2022', 2022, https://www.cyber.gov.au/about-us/reports-and-statistics/commonwealth-cyber-security-posture-2022. The report noted that only 49% of government agencies 'exercised their Incident Response Plan at least every two years'.
[99] ASD, 'Redspice', https://www.asd.gov.au/about/redspice.
[100] Department of Home Affairs, Review of the Migration System, 'Final Report', March 2023. https://www.homeaffairs.gov.au/reports-and-pubs/files/review-migration-system-final-report.pdf.
[101] Productivity Commission, 'Closing the Gap', website, https://www.closingthegap.gov.au/national-agreement/targets

accessed 11 April 2023.
[102] 'National Agreement on Closing the Gap', 2020, https://www.closingthegap.gov.au/national-agreement/national-agreement-closing-the-gap.
[103] 'National Agreement on Closing the Gap', 7B. Data Development Plan, https://www.closingthegap.gov.au/national-agreement/national-agreement-closing-the-gap/7-difference/b-targets/data-dev.
[104] ACSC, 'ACSC Annual Threat Report 2022', p. 47, https://www.cyber.gov.au/sites/default/files/2022-11/ACSC-Annual-Cyber-Threat-Report-2022.pdf.
[105] Department of Home Affairs, '2023-2030 Australian Cyber Security Strategy', undated, https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/strategy/2023-2030-australian-cyber-security-strategy.
[106] ACSC, 'ACSC Annual Threat Report 2022', p. 11.



CONTACT

info@socialcyber.co

www.socialcyber.co