SOCIAL CYBER INSTITUTE

Research Paper 2/24

AUSTRALIA'S CYBER SURGE:

THE MOTIVATIONS

Greg Austin

NOVEMBER 2024

Australia's Cyber Surge:

The Motivations

Greg Austin

November 2024

About the Author

Professor Greg Austin has diverse international experience in cyber policy research and international security policy: co-founder of the Social Cyber Institute, Senior Fellow and head of the Program on Cyber Power and Future Conflict with the International Institute for Strategic Studies (IISS) and Professor of Cyber Security, Strategy and Diplomacy with the University of New South Wales Canberra. His career, including a Senior Visiting Fellowship in the Department of War Studies at Kings College London, has included thirteen books on international security, as author or editor, and leadership of several international research projects. He is currently an adjunct professor in the Australia-China Relations Institute at the University of Technology Sydney. His service as a research leader for prominent global NGOs, such as the International Crisis Group and the EastWest Institute, has seen him work from Brussels and London. He has partnered with leading governments at Ministerial or senior officials level (Russia, China, UK, India, United States, Turkey, Australia). He has undertaken joint activities with major international organisations at leadership level (United Nations, International Atomic Energy Agency, R20 for Climate Action, World Customs Organisation). He has consulted for the UK Cabinet Office, the UK Ministry of Defence, the Foreign and Commonwealth Office, the European Commission, and the Australian Department of Foreign Affairs and Trade. 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.

Acknowledgments

The author would like to thank three reviewers for their comments on the draft.

Abstract

In March 2022, Australia announced the biggest expansion and upgrade of its cyber capabilities for national security and intelligence at any time since creation of its national-level signals intelligence organisation in 1947. In 2024, the government announced a superseding capital investment program in cyber and space platforms that appeared to be more than double the 2022 commitments in that budget category. The Russian invasion of Ukraine in February 2022 provided a political opportunity to announce the initial radical surge in spending but that war was not the main cause of the expansion. Announcements by the government on the purposes of the surge have been quite apolitical and reveal a heavy focus on what advancing technologies might dictate in intelligence and military affairs. The implied message was that Australia needed to do more to keep up with its major allies in cyber capability. In political terms, there were likely three main geopolitical motivations or drivers for the Australian cyber surge: containing foreign interference in Australia, the need to deliver new levels of cyber operations as part of the AUKUS reorientation and strategic uplift, and the government's exaggerated view of deteriorating strategic circumstances in the Indo-Pacific. The scale alone of Australia's cyber surge dictates a corresponding doubling of effort in oversight of ASD activities by parliament and the public, especially in respect of the agency's apparent intent for expanded operations inside Australia.

Contents

Introduction

Australia is undertaking the biggest expansion of its cyber capabilities for national security and intelligence at any time. While there had been a steady upgrade underway beginning in 2016, it was in March 2022 – just weeks after the Battle for Kyiv began – that the government announced a doubling of resources for the Australian Signals Directorate (ASD). The effort was labelled Project Redspice and committed an additional $10 billion over a decade.[1]

ASD is a joint civilian and military organisation that undertakes military and non-military cyber-related and signals intelligence activities largely through covert means. ASD retains lead responsibility for military and non-military cyber operations, both offence and defence, with the ADF responsibility lying mainly in the 'raise, train and sustain' function, while contributing to the development of strategy for cyber operations in armed conflict.[2] Historically, the remit for ASD activity was an external one, that is outside Australia.

A modest expansion in non-ASD cyber spending in the defence portfolio had already been underway following the creation of the Information Warfare Division in the ADF in 2017 and consequential activities.

In 2024, the government announced a massive capital investment program in defence cyber efforts that appeared[3] to be more than double the size of that budget category previously implied by Project Redspice's $10 bn boost. This new commitment included a $32 bn capital development effort over the coming decade in cyber and space, of which 'warfighting networks will benefit from $15 billion to $20 billion in the cyber domain, including defensive and offensive capabilities to fight malicious activity'.[4] The capital component of the Redspice commitment was only of the order of $6 bn (about $600 mn per year on average), judging by 2023 and 2024 budget estimates.[5] Sitting somewhere in this $32 bn announced in 2024 would be 'about $2.7 billion to $3.7 billion' for electronic warfare development and integration.

This paper looks at the geopolitical and domestic motivations for the continuing cyber surge and the intelligence assessments underlying it. How much was the Russia/Ukraine war a catalyst for the cyber surge and how much was it a convenient opportunity for much larger expenditures and a radically enhanced cyber posture in reaction to threats apart from Russia? The paper also analyses the link between the geopolitics of the cyber surge with the development of national cyber policy, looking at an apparent disconnect between the scale of the upgrades in capability and a relatively muted stance in public presentation of the seriousness and urgency of some of the threats[6] while exaggerating others.

The paper sets out the government's statements around the development of cyber capability between 2016 and 2024, concentrating on the announcements since the sharp and large-scale escalation of the Russia/Ukraine war in February 2022. The second part of the paper looks at alternative explanations of likely motivations (complementary influences) for the surge.

From incremental growth to surge

In 2020, this author criticised the Morrison government in Australia for incremental and inadequate funding of national cyber capability after it announced an uplift program valued at $1.35 billion over ten years.[7] On 20 February 2022, four days before the further Russian invasion of Ukraine, the Foreign Minister restated

similar information on spending plans for ASD, though with a slightly higher figure: Australia would be "investing $1.67 billion over 10 years to build new cybersecurity and law enforcement capabilities".[8] This pointed to some modest growth (about 25%) between the level of commitment announced in 2020 and the Foreign Minister's statement on the eve of the invasion.

This plan would be overtaken in March 2022, just weeks after the invasion, by the announcement from the Morrison government of Project Redspice for a total of $10 bn for new investments in cyber capability over ten years. This represented an increase in expansion plans by a factor of around seven between the uplift announcement in 2020 and the 2022 Redspice announcement, both over a similar period.

This Redspice commitment was immediately visible in the annual budget statement the same month it was announced (March 2022). Effectively, the expansion plans provided for a doubling: in February 2022, the annual spend for 2021-22 (by 30 June 2022) was expected to reach $1.157 but by the time of the budget for 2023-24, issued in May 2023 by the successor ALP government, the annual budgeted spend had climbed to $2.475 bn.[9] Table 1 shows the changes reflected in actual and planned spending between 2019 and 2028.

The large growth rate of actual budget spend by ASD between FY2019-20 and FY2023-24 of 200% has to be noted. For the sake of comparison, growth between 2019 and May 2023 in the overall Defence Budget in Australia (of which ASD is a part) was only 23%.[10] So the ASD budget growth rate between 2019 and 2023 outpaced overall defence budget growth by a factor of eight.

Table 1: ASD Budget Allocations by FY

2019-20 actual	$0.944[11]	Oct 2020
2020-21 proposed	$1.034[12]	Oct 2020
2021-22 proposed	$1.061[13]	May 2021
2022-23 proposed	$1.666[14]	Mar 2022
2022-23 actual	$1.715[15]	May 2022
2023-24 budgeted	$2.475[16]	May 2023
2023-24 actual	$2.859[17]	May 2024
24-25 proposed	$2.726[18]	May 2024
25-26 proposed	$2.471[19]	May 2024
26-27 proposed	$2.465[20]	May 2024
27-28 proposed	$2.214[21]	May 2024

On the basis of Redspice, the ASD planned to change at scale and speed.[22] The new policies were described by the government as the 'largest ever investment in the intelligence and cyber capabilities of ASD'.

Announced purposes

The policy document, likely drafted before the Russian invasion of Ukraine, did not mention that subject. It identifies the centrality of cybersecurity to modern warfare and adopts an offensive approach to defending critical infrastructure. It directly aims at delivering asymmetric strike capabilities and offensive cyber for ADF and will invest in next generation data science and AI capabilities.

When it was announced, the funding priorities for Redspice were presented as a tripling of offensive cyber capability, a doubling of persistent cyber hunt activities, a gain of 1900 new posts in cyber operations over the decade, an ambition to have 40% of staff located outside Canberra,

and a quadrupling of the global footprint (whatever that might mean precisely).[23]

For comparison's sake, US intelligence agency spending under its two main programs for which reporting is available (a total sum for the main agencies of which only one was the National Security Agency) remained relatively stable over the past decade.[24] Cyber Command benefited from a budget reorganisation that saw it win a budget hikes in beginning in US FY 2022 (with corresponding reductions elsewhere in the armed forces).[25]

In 2023, the ambitions of ASD for its expansion and upgrade under Redspice focused on five priorities, all aimed at positioning Australia better for strategic advantage over its potential adversaries:

- offensive cyber, especially for the ADF
- more reliable strategic warning and higher quality intelligence
- better critical infrastructure defence
- more resilient classified communications capabilities
- expansion of the domestic operational footprint.[26]

Of these, the most surprising is the last one: an expansion of domestic operations. It can be read alongside the third point ("better critical infrastructure defence"), which also has a clear domestic focus. This will be discussed later. Less surprising is the elevated commitment to offensive cyber in military operations. This will also be discussed later.

To get some sense of potential items of expenditure of the Redspice investment, it is useful to compare the ASD budget proposed in May 2023 with the March 2023 budget request for US Cyber Operations at US$1.318 bn, with an additional US$332 million for Cyber Command.[27] We would not necessarily expect close alignment, but the details for the US are useful for appreciating its view of important areas of increased cyber operational expenditure. The two countries do not have completely parallel systems and priorities but they do operate in cyberspace with similar strategic interests and shared adversaries. We should also note that US Cyber Command has narrow defence (military) interests as its core mission, compared with the US National Security Agency (NSA) which is the core cyber intelligence agency (as ASD is for Australia).

In that US budget request, program growth was most notable in these categories set out in Table 2.

Table 2: Cyber Command FY 24 Budget Request (March 2023)[28]

Category	Cost (US$m)
USCYBERCOM Civilian Workforce Pay	62.057
Joint Operations Support Program	46.400
Cyberspace Support	43.873
Cyber Training	39.611
Increased Cyberspace Efforts (Climate and Pacific Deterrence Initiative)	32.618
Enhanced Sensing and Mitigation	26.000
Cyber Readiness Support and Integration	24.500
CMF, CO-IPEs, and JFHQ-C Civilian Pay	23.548
Operational Response Platform	22.200
Cyber Protection Team Support	18.000
Cyber Protection Team Defense Mission Support System Kits	15.687
Hunt Forward Persistent Engagement	15.100
Total	**369.954**

Notwithstanding several large differences in mission and funding levels between the US Cyber Command and ASD, the categories of spending upgrade in the list above might have some reasonable alignment with those of ASD. For example, ASD recruitment over the decade of Project Redspice is planned at about 200 new per year (1,900 over the decade), along with salary raises in some categories. For 2022-23, ASD overperformed in recruitment, achieving a net growth of around 300 personnel. The NSA is currently on a recruitment drive which it began in 2023 for 3,000 new employees for each of 2023-24 and 2024-25. Table 3 gives some comparison of personnel strengths of various agencies, including the UK's GCHQ.

Table 3: Projected Personnel Numbers ASD, GCHQ, NSA/CSS and Cyber Command in approaching FY as of 2023 annualised data

	ASD[29]	GCHQ	NSA/CSS	CyberCom[30]
Civ FTE	2,605	>6,000	>20,000	>6,539[31]
Civ P/T	255	n/a	n/a	n/a
Mil (Reg)	n/a	n/a	n/a	518
Mil (Res)	n/a	n/a	n/a	79
Contractors	n/a	n/a	n/a	n/a

n/a = not available

Announcements by the Australian Defence Department in 2024 marked a dramatic new phase in national defence strategy, bringing it into line with US and UK concepts for warfighting, captured best in the centrality of the concept of 'decision advantage'. While the concept is specifically mentioned only twice in the Australian National Defence Strategy,[32] it does underpin all six capability effects on which the Integrated Investment Program is based.[33]

One of the 2024 documents added a rather long list of additional objectives of sub-aspects not so visibly promoted in previous statements:

- enhanced deployable defensive cyber operations capability for the ADF
- a comprehensive training program to support the growth of the ADF cyber workforce
- capabilities to better understand, operate in and secure the cyber 'terrain' improving the warfighting cyber capabilities of Defence's networks
- strengthening their cyber interoperability with the United States and other key partners
- developing joint warfighting networks and applications that will improve communications access for ADF forces operating in challenging environments
- strengthen network security and resilience
- enhancing strategic communications systems
- developing alternative position, navigation and timing capabilities
- modernising Defence's cryptography to provide enduring communications security.[34]

The investment increases newly announced in 2024 are reflected in Table 4.

Table 4: Investments in Cyber Capabilities in the 2024 Announcement[35]

	Approved Planned Investment (2024-25 to 2033-34)	Total Planned Investment (2024-25 to 2033-34)
Cyber capabilities	$1.4 bn	$6.4bn - $8.4bn
Cyber terrain	$1.9bn	$8.9bn - $12bn

This massive scale of the 2024 investment plan was foreshadowed only in general terms in the '2022 Defence Information Technology Strategy'[36] and in rather muted terms in the 2023 Defence Strategic Review except in two recommendations:

- 'A comprehensive framework should be developed for managing operations in the cyber domain that is consistent with the other domains'
- Defence's cyber domain capabilities should be strengthened to deliver the required breadth of capability with appropriate responsiveness to support ADF operations.

The 2024 changes were not foreshadowed in any meaningful way in a 2022 'Defence Cyber Security Strategy'.[37]

The annual growth rate in commitment to cyber-related spending in the 2024 Investment Program for the years 2024-33 appears to be 3-4 times greater than initially planned at the time of the Redspice announcement. The growth rate of several hundred per cent was also well ahead of the growth rate in the overall defence budget (53% for the period 2019-20 to 2024-25).

Domestic cyber security not the main driver

A review of the cyber front at home in Australia does not bear out a suggestion that more cyber defence on the scale foreshadowed by Redspice and subsequent announcements was needed domestically in what might be termed the fight for classic cyber security (protecting government and corporate IT systems, including critical infrastructure, from cyber intrusions by criminals or data theft by foreign states).

The available data from the Australian government on reported cyber incidents in Australia to which ASD responded between 2019 and 2023 (Table 5) does not show a dramatic increase, but actually shows a substantial drop in 2019-20, a modest rebound in 2020-21, and a decline again in 2021-22, to the lowest level in four years.[38] The data illustrates the very low number of incidents in the National Security sphere. In the financial year in which Redspice was announced (nine months into the FY), there had been zero incidents (to which ASD responded) affecting national security or systems of national significance. In that year, there had been a trebling of incidents affecting state agencies (from 35 to 104). The data may not tell the full picture depending on whether the descriptor 'incidents responded to by ASD' includes all major incidents.

Table 5: Incidents Responded To (number) by Target Type And Fiscal Year

Year	TOTAL	*Nat'l*	*Other Fed*	*State*
2018-19	2164	*6*	*71*	*23*
2019-20	1134	*27*	*108*	*31*
2020-21	1630	*9*	*58*	*35*
2021-22	1100	*0*	*61*	*104*
2022-23	1134	*12*	*84*	*12*

NAT'L = national security, systems of national significance
OTHER FED = federal govt, govt shared services, regulated CI
STATE = state govt, academia, large organisations, supply chain

In contrast, cybercrime incidents expanded and may have helped push the government to some expansion of ASD spending but likely far from enough to justify the scale of the Redspice spending. In its annual cyber security threat report (for the 2022 calendar year), the Australian Cyber Security Centre (ASCS) recorded 76,000 cybercrime incidents which is an almost 13% increase since the previous year.[39] This number is many times bigger than for ASD's category of 'incidents responded to by ASD'.

The 2022 threat report did directly call out Russia's use of cyber operations during the Ukraine war but the concerns expressed do not seem to match the massive surge in spending. The report did recognise that a key vulnerability Australia would need to defend would be cyber supply chains. Australian network owners would also need to secure critical systems through improved segmentation between corporate and operational networks.

Prior to REDSPICE, as mentioned above, the government had already pledged $1.35 billion to security agencies as part of a Cyber Enhanced Situational Awareness and Response (CESAR) package, which was aimed at securing civil services and public infrastructure.[40] Announced in 2020, the CESAR package was aimed at boosting protection and cyber resilience for Australians at an individual and business level. $31 million was allocated to disrupt cybercrime, $35 million was targeted towards a cyber threat-sharing platform, $12 million was aimed at strategic mitigation and active disruption. Therefore, while Australia was already doing quite a lot to securitise its cyber architecture since before the Battle for Kyiv. With project REDSPICE the available budget doubled. In 2022, the incoming Minister for Home Affairs and Cyber Security announced that the 2023-2030 cybersecurity strategy would provide the sea change that Australia needed to better improve its national resilience. The strategy announcement also stated the Government's vision to ensure that Australia becomes the world's most cyber secure nation by 2030.[41] The strategy also aims to address criminal intrusions into Australia's health and telecommunications sector and has prioritized the protection of critical infrastructure.

As part of the strategy, Australia has also proposed 6 cyber shields that it aims to set up by 2030.[42] The first includes long-term education to ensure that citizens understand cybercrime and disinformation and can take active measures to protect themselves. The second is to ensure the proliferation of safer technology and a quicker recognition process for identifying insecure software. The third shield is connected to threat-blocking and intelligence sharing. It hopes to establish means to ensure real time data exchange on malicious attacks and actors. The fourth shield is aimed at the securitization of critical infrastructure. The fifth shield is the development of sovereign capabilities through increased development of cyber skills amongst the youth and to foster a cyber skilled workforce. The sixth shield is global coordinated action to ensure the establishment of a resilient cyberspace.[43]

Geopolitical Motivations

It is possible that the commitment to such radical increases in cyber investments announced in March 2022 and subsequently was stimulated by Russian cyber operations against Ukraine both over the preceding decade and as they escalated in mid-2021 through to the Battle for Kyiv and continuing war by Russia in Ukraine. There are three alternative and more likely causes explanations with a high degree of complementarity between them: domestic security needs to defeat foreign interference, imperatives of AUKUS, and as a lesser concern, the more threatening cyber military postures of China and Russia.

Internal Security Needs

The Redspice cyber surge announcement in March 2022 was likely part of the governing Coalition's re-election bid, coming as it did

just one month before the Prime Minister announced on 10 April 2022 the election date of 21 May, the latest possible date it could be held under Australian constitutional practice. The decision emerged in an environment where a series of political scandals had driven electoral support well below winnable levels for the coalition Liberal National Party (LNP) government and it may have felt that additional security spending on this scale may help it in the election.

The most important was a growing fear of covert foreign influence and disinformation in Australia that were either enabled by or more easily addressed by cyber technologies. This would entail better monitoring by ASD (working in support of ASIO's execution of its remit for internal security and in support of ASIS and DFAT in their remit for foreign intelligence collection on these interference efforts). The previous government had received an intelligence assessment in 2021 that 'for the first time ever', the 'biggest national security challenges that we face as a country are espionage and foreign interference'.[44] It is largely for this reason that the Labor government elected in May 2022 gave its Minister for Home Affairs a secondary role as Minister in the Defence portfolio, a practice continued under a Ministerial reshuffle in August 2024.

The former Defence Minister, Peter Dutton, who had led the new cyber announcements in 2022 was the same person who had been the Home Affairs Minister in 2019 and 2020 advocating publicly for a 'sensible discussion' of expanding ASD powers to operate in Australia.[45] He may have also led the discussion in the Cabinet in 2018 on the same topic when it was reported that the Prime Minister of the day, Malcolm Turnbull, had rejected the idea. By 2020, after Turnbull lost the Liberal Party leadership, Dutton was able to claim some success relying on the need to be able to stop international cybercrime, especially sexual abuse of children. In the period up to 2020, the LNP Coalition government had introduced a series of reforms to domestic cyber surveillance and telecommunications interception in the name of counter-terrorism needs, which some Australian scholars and international journalists had labelled the most draconian in any liberal democracy.[46]

One of the notable elements of the Redspice announcement was an expanded domestic orientation, a continuation of the shift away from the once exclusively non-domestic remit of ASD's predecessors. Even today, ASD still mentions 'foreign intelligence' on its website as a primary focus,[47] traditionally imagined as collecting information 'beyond the water's edge' and not inside Australia. This is a distinction still maintained between Australia's domestic security agency, ASIO, and externally oriented Australian Secret Intelligence Service (ASIS). But the Redspice announcement made little of that distinction because the contemporary needs of signals intelligence and cyber operations permeated all domestic security interests. This can be seen in the articulation in Redspice of the five ASD objectives:

1. Generate intelligence and operational effects to protect and advance Australia's national interests
2. Make Australia the safest place to connect to the online world. Foster national cyber security resilience
3. Enable the war fighter. Protect Defence personnel and assets
4. Protect Australia and Australians by countering cyber-enabled crime and disrupting terrorists' use of the internet
5. Deliver timely, trusted and quality advice to Government, law enforcement, business and the community.[48]

An important aspect of the evolution of ASD and the country's cyber posture has been the constant process of review and

legislative reform since 2001. Between then and the end of July 2019, the Parliament passed 124 laws making major (non-technical) amendments to the legal regimes for the national intelligence community, including many affecting ASD.[49] There were more than 14,500 specific amendments. A number of these addressed the realisation, evident in Australian policy circles at least since 1976, that a distinction and demarcation in the intelligence community between foreign and domestic sources of threat had become 'less mutually exclusive'.[50] In practice, this had been addressed by working arrangements that saw the assets of the various agencies mobilised as needed in joint activities that respected the legal authorities relating to foreign or domestic intelligence activity. At the same time, an intelligence review launched in 2017 found that ASD had a broader role in information assurance and cyber security roles 'as well as the greater interdependencies' with the country's other intelligence agencies'.[51] ASD had in fact been operating a CSOC since 2010. On the other hand, as of 2020, the Intelligence Services Act limited ASD intelligence collection to the 'capabilities, intentions or activities of people or organisations outside Australia'.[52]

In 2023, the Labor government introduced legislation to modernise these legal authorities more comprehensively than the LNP government had between 2020 and 2022. Specifically, the new Act provided a new regime for authorising ASD to collect intelligence on Australian citizens in certain circumstances, especially where there is a national security threat. The authority in any case would subject to approval by the Defence Minister (who is responsible for ASD) and the Attorney General.

After the Redspice announcement, Australia suffered some of its most serious cyber attacks, mostly by criminals,[53] which might have provided *post facto* vindications on the domestic front for the cyber surge beginning in March 2022, but they have not been the cause. In recent years ASIO has publicly revealed a number of foreign intelligence operations inside Australia which have almost certainly depended on ASD surveillance operations of Australian citizens. For example, in a 2024 announcement, ASIO identified Australian citizens as targets of its surveillance in connection with an Indian intelligence operation since 2020.[54] These Australians would have been surveilled largely through ASIO legal authorities, including for telecommunications interception, but ASD would have been able to provide information collected through its normal operations. The Australian surveillance targets included 'an Australian Government security clearance holder with access to sensitive information', 'current and former politicians', 'Australians with access to privileged and classified Information', and 'community leaders who favoured the foreign agency's Agenda and monitored their country's diaspora community'.

Effective public scrutiny of ASD's allocation of resources to the cyber security mission would appear to be urgent. The appointment of a new Director General ASD to take up the role on 6 September 2024 presents an ideal opportunity to reconsider performance. On the one hand, we should not expect ASD to deliver cyber security for the country, it can only provide a good policy environment and a range of support services for the private sector, community organisations and citizens. On the other hand, ASD and the Australian government have been too timid in standard setting for cyber security performance by government agencies and large corporations. The culture of cyber security in Australia needs urgent attention. A move in this direction was made in July 2024 when the government announced three new urgent measures that seemed overdue in their very nature: 'identify indicators of Foreign Ownership, Control or Influence (FOCI) risk as they relate to procurement and maintenance of technology assets and appropriately manage and report those risks'; a 'technology asset stocktake on all internet-facing systems or

services'; and a mandate to share all threat intelligence with ASD.[55]

The challenges to ASD in its national cyber security policy mission are however much bigger in non-government agencies than in the government. ASD has, appropriately, had to weave a fine line in recognising private sector interests in limited regulation while imposing some measure of additional oversight and control through legislation. It is probably hard to fault the way in which the government and ASD have conducted themselves in the past two years in manging this balance. One legislative distillation of how aspects of this will be managed came in the form of 2024 Act on National Security Legislation Amendment (Comprehensive Review and Other Measures No. 3).[56] The law enacted or otherwise addressed a number of reforms recommended by the Richardson review into the legal framework intelligence.[57] These reforms have been complex and in sum represent a considerable advance in public policy. There have been critiques on civil liberties issues, privacy rights and ambiguities in definition which have not been reflected in the legislation but which ASD should not now overlook in how it frames the public presentation of its domestic operations.

One point of framing may need to be given more attention. Australia (like its allies) cannot do a lot to shape the cyber threat environment. We can try to raise costs for attackers where possible, or actually block their efforts, but the bad actors, not the Australian government, set the threat environment. There is a wide consensus among our allies that the threat levels are escalating and will continue to do so, particularly from Russia and China, but also from criminals, in spite of increased levels of security by the target countries like Australia.

AUKUS Reorientation and Strategic Uplift

The cyber surges of 2022 and 2024 can best be understood as part of the overall stiffening of Australian national security capabilities underway for almost a decade and a new focus on military cyber capabilities since at least 2017 when the country set up its new Information Warfare Division in the armed forces.[58] In July 2020, Australia released a Defence Strategic Update and a Force Structure Plan for the Australian armed forces, followed by a Cyber Security Strategy in August of that year.[59] These documents reflect an increased awareness of military cyber threats and opportunities, a sustained commitment to ongoing reforms, and a more rapid pace of implementation of these changes along with supporting financial investments as discussed above. Prime Minister Scott Morrison emphasized the importance of new cyber strike capabilities as essential for a robust deterrent strategy. Notably, these military policy documents prioritize enhancing information and cyber capabilities over traditional military domains such as land, sea, and air for the first time. Collectively, the two defence documents signal a significant shift towards recognising that 'information is fundamental to all effective military operations', despite the government and the Australian Defence Force avoiding the term 'information dominance' as used by the United States.

In 2021, Australia embarked on a radical new strategic direction in the form of the AUKUS agreement of that year which has two pillars.[60] The first would see the country acquire nuclear-powered submarines from its AUKUS partners. The second pillar would focus on trilateral development of 'cyber capabilities, artificial intelligence, [and] quantum technologies'.[61] The overall goals of AUKUS include 'deeper information and technology sharing' and 'deeper integration of security and defines-related science, technology, industrial bases, and supply

chains'. To achieve both of these (submarine acquisition and technology gains), Australia would need to radically ramp up its investment in military cyber technologies, especially for sub-surface warfare and related intelligence collection and war-fighting needs.

After February 2022, the Australian government announced significant adjustments in cyber military policy (moving from 'joint warfare' concepts to 'integrated warfare', embracing strategic cyber strike, and investing much more heavily in cyber capabilities).[62] The most dramatic change in cyber posture was the release in March 2022 of Project Redspice, as described above. The policy document adopts an offensive approach to defending critical infrastructure. It directly aims at delivering asymmetric strike capabilities and offensive cyber for ADF and will invest in next generation data science and AI capabilities. [63]

In late 2023, the Labor Party government (elected in May 2022) released an unclassified version of a strategic review it had commissioned, and it made integrated war-fighting capability across five domains (including cyberspace) the foundation stone of future planning.[64] It highlighted an 'enhanced long-range strike capability in all domains', including cyberspace. The statecraft underpinning defence posture would involve 'the reorganisation of elements of the national intelligence and national security community; substantial investments in cyber security; … and measures to resist foreign interference and protect critical infrastructure'.[65] The government agreed with all of the key cyber recommendations in the Review.[66] Neither Ukraine nor Russia are mentioned by name in the unclassified version of the Review, and Europe receives only one mention in passing, while China is mentioned nine times.

The government subsequently announced a review into Australia's intelligence agencies, and while casting it as a normal event, this action needs to be read against the expressed need for reorganisation of certain key elements.[67] The most recent overall review had been finalised in 2017, though an important review of related legislation had also been undertaken in 2019, and a public version released in 2020.[68] The latter review extended the power of ASD (along with ASISI and ASIO) to collect intelligence on Australians under certain specified circumstances, subject to the preliminary approval of the Attorney General.[69]

The 2023 Defence Strategic Review stated a new view that deterrence strategy and practice was evolving and that the country's strategy of denial had to include non-geographic threats, including cyber.[70] It also promoted larger investments and analysis in 'crucial future-focused joint capabilities such as information warfare, cyber capabilities, electronic warfare, and guided weapons and explosive ordnance', with corresponding changes 'to mindsets and technologies to deliver competitive advantage'.[71] The review recommended that Defence develop a comprehensive framework for 'managing operations in the cyber domain that is consistent with the other domains' and that cyber capabilities 'should be strengthened to deliver the required breadth of capability with appropriate responsiveness to support ADF operations'.[72] The analysis delivered a stinging critique of underinvestment in Defence cyber security and information technology policy, saying that the country's Tax Office appeared to be better structured and funded than the Defence IT management organisation, which had consistently under-performed in new project implementation.[73]

The adjustments in international cyber policy in the years preceding the Redspice announcement had seen corresponding changes in emphasis of Australia's cyber diplomacy away from a heavy focus on good international citizenship, especially under UN auspices[74] to a much sharper alliance-based diplomacy. This involved new types of

diplomatic activities organised around the Five Eyes Group, NATO and likeminded countries in ways meant to isolate countries like Russia and China for their unacceptable cyber activities and to strengthen allied operational military readiness in cyberspace.[75]

For example, on 20 February 2022, four days before the invasion, Australian joined with its AUKUS allies (the United States and the United Kingdom) in the attribution to Russia military intelligence of cyber attacks against the Ukrainian banking sector several days earlier.[76] The statement called out 'solidarity with Ukraine and our allies and partners to hold Russia to account for its ongoing unacceptable and disruptive pattern of malicious cyber activity'. It said that Russia's cyber actions pose a 'significant risk to global economic growth and international stability'. Australia undertook a public attribution of cyber attack to Russia as early as 2018[77] as part of a policy shift that began in 2017.

One immediate lesson of the Russia/Ukraine war was the need to be more flexible about international cyber relationships than in the past when the Five Eyes countries had jealously guarded their cyber-based intelligence and cyber defence capabilities. It was a private and exclusive club. Prior to the direct intervention of the US in Ukraine's cyber defence in 2021, prior to the Battle for Kyiv, Russia had no good reason to believe that the US, supported by its allies, would effectively blunt most Russian military and political objectives through cyberspace operations (especially intelligence collection whose product was shared with Ukraine). After all, Ukraine was not even a member of NATO and had not been identified as a reliable cyber partner given that the country was a hotbed of cyber-crime and that its government agencies had been seriously compromised by Russian intelligence assets. As for timing, the scale of the US cyber intervention in Ukraine and its military significance through the course of 2021 would have been well known to the Australian government. The subsequent course of the war, and the success of US and allied cyber interventions, effectively rewrote the playbook for cyber diplomacy by the Five Eyes countries.

In 2023, Australia participated in the Locked Shields exercise run annually by the NATO Cyber Cooperative Defence Centre of Excellence (CCDCOE) for the first time, having announced its intention to join the Centre in 2018.[78] The Department of Defence began to lay the ground-work for stronger regional partnerships in cyber security by translating introductory guides on the subject into 20 regional languages.[79] This complemented a modest programme of cyber security capacity building in the region in place for five years, as part of an active programme of globally oriented cyber diplomacy under its cyber ambassador appointed in 2017.

By 2024, Australia extended the scope of its cyber diplomacy by going well beyond the traditionally exclusive confines of the Five Eyes group when it joined 15 other countries, alongside FVEY partners, to publish 'Guidelines for secure AI System Development'.[80] The new partners for the Five Eyes in this included Chile, Czechia, Estonia, France, Israel, Italy, Japan, Norway, Poland, Singapore, South Korea, and Sweden. This was part of Australia's more robust international cyber engagement in response to the pace of technological change, the growing complexity of cyberspace, and escalating tensions with Russia in cyber affairs. Leading private sector companies and advanced research centres also contributed to the publication.

The government's National Defence Strategy in 2024 committed to long-term investment in cyber capabilities that strengthen situational awareness, the ability to project force and decision advantage'.[81] It elaborated on the goals as follows:

- enhanced intelligence, surveillance and reconnaissance
- resilient communications
- computer network 'defence and disrupt' options
- an uplift to Defence's communications networks
- greater network efficiency, resilience and redundancy
- enhanced defensive cyber capability through investment in workforce and cyber mission systems.[82]

By August 2024, Australia's military cyber transformation arrived at a new level when it announced the formation of its first formal Cyber Command using that appellation.[83] In announcing the change, Defence said that the ADF has 'renewed its focus on cognitive and information warfare'. It observed that the move 'continues the acceleration towards an integrated, focused force' and allows the delivery of 'effects within the information environment, which encompasses all five domains'…. 'The cyber domain plays a critical role in force generating cyber power and information advantage capabilities'. The new Cyber Command appears to have been built out a pre-existing Sigint and Cyber Command and a separate Cyber Warfare Division in the Joint Capabilities Group but it also took over single service cyber units, a Cyber Forces Group, and the Joint Public Affairs Unit.[84] The newly badged Cyber Command would operate in parallel with the 'Cyberspace Operations Division,[85] Joint Capabilities Division,[86] Strategic Military Effects Branch[87] and ADF personnel employed within the Australian Signals Directorate'.

This evolution, though episodic and subject to regular institutional adjustment, was more or less predetermined from 2017 when the first Information Warfare unit was set up in the Australian Defence Force.

Deteriorating strategic circumstances

The discussion above identifies two main reasons for the cyber surges in Australia in 2022 and 2024: countering foreign interference and keeping pace with key allies in cyber modernisation and expansion of cyber forces. In this analysis, the strategic circumstances most relevant were covert operations inside Australia, not the preparation for war by China against Taiwan at some unidentified time in the future nor the Russian war against Ukraine already underway since 2013 or 2014. This section of the paper offers some additional perspective on whether the cyber surge after March 2022 was premised on the increased likelihood of imminent war involving Australia (that is, strategic circumstances outside Australia).

Prior to the Redspice announcement in March 2022, the LNP government had created an alarmist atmosphere in public policy premised on the judgement that Australia should adjust its military preparations and readiness level for an increased possibility of war.[88] This grim assessment was based in part on elevated concerns about foreign interference in Australia, including influence operations enabled by cyber technologies. But it was part of an escalating scare campaign put in place by key figures in the LNP coalition government, several think tanks, and some scholars, and not significantly de-escalated after the change of government in May 2022 to the Labor Party.[89] In fact, in simply carrying on with the sensationalist claims the new government defied its Labor Party heritage of being more balanced in such matters than its LNP opponents. This was particularly in evidence when the new Labor government repeated verbatim false claims from the LNP that China had undertaken the largest military buildup of any country since 1945.[90]

An associated claim about the urgency of Australia's strategic predicament as a possible driver of the cyber surge was the elimination of what was alleged to have been a ten-year window of warning time for major conflict. In launching the new National Defence Strategy in April 2024, the Defence Minister, Richard Marles said: 'Australia no longer has the luxury of a ten-year window of strategic warning time for conflict.'[91] He claimed in the next sentence, that 'the combined effect of this [the non-transparent military build-up by China, the Russia/Ukraine War, Middle East War and China's actions in the South China Sea] has seen our strategic environment deteriorate over the last twelve months'.

The claim of non-transparency is reasonable in terms of very few details contained in Chinese public statements, but the Chinese buildup is thoroughly documented in unclassified US intelligence, US Defense Department reporting, and regular assessments by the Congressional Research Service. Few of these assessments repeat the line of the Australian government about the biggest military buildup of any country since 1945.

In fact, prior to the Redspice announcement of 2022, little had changed in Australia's immediate environment in the previous twelve months or even the previous two years in respect of China's strategic operations of high interest to Australia. China's defence modernisation continued on pre-established trend lines. Its operations in the South China Sea continued to expand, with a new focus on operations near Indonesia's Natuna Island.[92] A joint military exercise with Russia in the area had been commonplace since 2012.[93] The main negative change had been a temporary surge in military air patrols by China beyond an unofficial median line in the Taiwan Strait in 2020, and an expansion of similar occasional operations in areas to the southwest north and east of Taiwan.[94] On the other hand, there had been positive changes in China's strategic actions as well, including from the Australian point of view. At the time Marles made the speech, Australia was already planning to host China's Premier to mend the stand-off and antagonism between the two governments over several years.

In addition, the organising concept of ten-years' warning time had been explicitly abandoned by Australia in 2020 in its Strategic Update under the LNP government,[95] even though its claim that it had been a central concept for defence planning before then is a dubious one. The government in 2024 is both dissembling and relying on ambiguity about the concept of warning time. For example, the 2016 White Paper does not mention warning time. In the 2013 White Paper, the concept had been used to refer to 'warning time' for the development of capabilities for major attack on Australia, not merely any armed conflict affecting Australian interests, as Marles is using the term in 2024. The 2013 White Paper said:

> Potential adversaries may have capabilities that can reduce the protection provided by distance and thereby reduce our early warning and mobilisation timeframes. At the same time, Australia's Alliance and regional defence partnerships play a valuable role in helping us shape the strategic environment to reduce, deter and deal with these threats if required, complementing our self-reliant capabilities. We would still expect substantial warning time of a major power attack, including dramatic deterioration in political relationships.[96]

Nevertheless, the 2024 claim about change in warning time, was already two to four years old by the time of the announced

cyber surges in 2022 and 2024. If the 'warning time' change occurred in 2020 and it was relevant to cyber force structure, why did Australia not undertake a cyber surge of similar scale in 2020 or 2021?

As noted earlier in this paper, there had been a mini-cyber surge in 2020, with the government announcing $1.5 bn spend on cyber capabilities and operations over the coming decade without making clear what part of that would be new spending that had not been previously announced.[97] The amount would include $470 million spread over ten years to increase the cyber workforce by more than 500 new Australian jobs over the decade. This level of funding was described the government at the time as the 'largest ever investment in cyber security' by Australia. At that time, this author had argued that the levels of new investment in cyber capability announced in 2020 were seriously inadequate.[98]

The most compelling argument against the idea that the cyber surge was part of a deliberate element of national preparedness for imminent war or seriously deteriorating strategic circumstances is the relatively slow pace at which constituent components of it were being put in place, especially ADF recruitment and training. For example, the decision to set up a Defence Cyber College was in place by 2019, its construction began in 2021, its first courses were offered in 2023, but its curriculum was still being developed in 2024. (The college, a joint effort by ASD and the ADF, probably represents to some degree a degree of continuation of pre-existing training by ASD, but few details beyond these just mentioned are publicly available.)

Another argument about the lack of urgency can be found in the government's prevarication in procurement of new submarines to replace its very old Collins class submarines. The initially proposed timing was to have the first new submarine in service in 2040 even though fleet to be replaced was to have begun retirements in 2025.[99] So at the same time as Australia was making its first cyber surge in 2022 it was proposing a two-decade delay in acquisition of new submarines considered vital as part of its strategic posture.

In fact, it is likely that the cyber surge beginning in 2022 was only made possible by the projected expansion of the ten-year defence spend announced in 2020 to $575 billion, up from $447.6 billion foreshadowed in the 2016 Defence White Paper (a nominal increase of almost 30%).[100] Of note, the 2020 Strategic Update encapsulated the strongest rhetorical commitment to date by an Australian government of the role of cyber operations in modern warfare and deterrence, with the government (specifically the Prime Minister Scott Morrison) talking of its stand-off strike potential for the first time.[101] It was 2020 that the ADF issued a new doctrine for cyber operations that has remained classified.

The strategic circumstances of Europe were likely not a driver of the 2022 or 2024 cyber surges by Australia. Russia had already seized the Ukraine's Crimea region in 2014 beginning with a covert insertion of troops and a manipulated referendum in Crimea on secession of the territory from Ukraine. Russia also set in train an armed insurgency in two other eastern provinces of Ukraine (Donetsk and Luhansk). This became the largest, best-armed insurgency in Europe since the end of the Second World war. Most importantly, Australian passengers had been killed when a Russian soldier shot down MH17 on 17 July 2014, an event that led to political confrontation between Australia and Russia, talk of sending Australian troops to the crash site, and (we can presume) inevitably heightened cyberspace operations by each side against the other. This cyber reality was intensified when Russia sent a naval intelligence collection ship to the Coral Sea in support of the Russian's President's participation in the 2014 G20 summit hosted by Australia.[102]

The second Russian invasion in February 2022 quickly became the largest war in Europe since 1945, surpassing in levels of violence and numbers of deaths the Soviet invasion of Czechoslovakia in 1968, the Yugoslavia wars of the mid-1990s, the NATO/Serbia war in 1999, or the war second Chechen war in 2000. But Australia did not in those decades or in the 2020s see European wars as a catalyst for Australian force structure changes.

The Russia/Ukraine war after February 2022 has differed in one major characteristic from those earlier European military crises or wars. In the Russia/Ukraine war, the US has committed itself to the defeat of Russian forces through the provision of advanced intelligence, military training and equipment to Ukraine. It has also set itself the objective of weakening Russian strategic power so that it cannot again launch such an aggression against another state.[103] The UN General Assembly passed a resolution condemning the Russian act as aggression and therefore a grave violation of the UN Charter.[104] The Australian government voted for the UN Resolution and has consistently supported its main elements. Australia has provided Ukraine with some military assistance, priding itself as one of the most important non-NATO donors.[105] Australia will have been particularly concerned that on the eve of the Battle for Kyiv, the Presidents of Russia and China met to declare a 'no limits strategic partnership'.

On the other hand, while the new phase of the Russia/Ukraine war represented a major deterioration in Australia's strategic circumstances, Australian strategic policy was becoming concentrated on a potential strategic crisis in Asia and most specifically a war involving China well before the 2022 Battle for Kyiv. Therefore, Australia's pre-invasion rhetoric on cyber threats and appropriate responses needed little change in response to the Russian invasion of Ukraine and the Battle for Kyiv. In 2021, with China's military modernisation and more intimidating military posture in mind, the talk by Australian leaders about the most serious threat to Australia's security environment since 1945 left them little place to go after that in terms of broad strategic policy pronouncements describing the gravity of the international threat environment. The Russian aggression led to new urgency in NATO for its members to actually meet their commitment to raise defence spending to 2% of GDP and this gave new political cover to Australia to increase its defence spending, even though it was already hovering around the 2% mark.[106]

A key question about the motivations of the Labor government that came to power in May 2022 is whether it believed the lines it was using about the deteriorating strategic circumstances ('worst since 1945', 'China's military buildup the 'biggest by any country since 1945', and the loss of warning time for conflict). The answer would likely be that since the previous LNP government had invented these lines of argument (based presumably on intelligence advice), the Labor leaders would have seen little reason to review them or change them.

The lines of argument have not been questioned directly as to their substance by any significant strategic analyst even though there have been may senior figures in the foreign policy field calling on the country to be less confrontational toward China and arguing that China was not as serious or imminent a military threat to Australian military circumstances as the Labor and LNP governments had been making out.[107]

Conclusions and Questions

Compared with its US counterparts, ASD practices for public disclosure of its activities remain on the conservative side, in spite of its moves in the past decade to more openness. In these circumstances, given the

lack of detailed information due to secrecy concerns, there are few reliable benchmarks for assessing the adequacy of the ASD spending growth. This author is nevertheless comfortable with the broad direction and scale of the effort under the cyber surge, though shortcomings remain and will take a decade or more to address.

If we restrict an assessment of Australia's cyber surge beginning in 2022 to our understanding of what was needed for just the traditional mission of ASD (intelligence collection on foreign targets), we could reach the conclusion that it was likely overdue by eight to ten years. By 2011, the trend in expansion of Chinese diplomatic, economic and military power was firmly in place, so much so that Australia supported the US 'rebalance to Asia' as an important hedge against a potentially more hostile environment. This included stationing of US forces in Australia to begin the following year. Vietnam had began reclaiming land on occupied South China Sea islands to fortify them. It was also 2011 that the US National Counter-Intelligence Executive called out significantly elevated levels of Chinese cyber espionage.

As concern rises about such shifts in a country's strategic environment, the first area in which a government should invest more money has to be national security intelligence, including signals. For Australia, the main aim is to support assessment of foreign strategic threats, especially to obtain the maximum warning of developments that might conflict with Australian interests.

In addition to collection of intelligence on policies and intent of foreign governments, there has been a growing need for improved counterespionage against rapidly proliferating cyber data exfiltration by China, Russia, North Korea and Iran, not to mention some countries traditionally friendly to Australia.

This traditional mission of ASD has also included reporting on threats of foreign influence inside Australia and the agency appears to be doing well on that front.

There has also been the widely accepted ASD mission of supporting counter-terrorism operations by ASIO and the AFP inside Australia through signals intelligence collection, as terrorist attacks and foiled plots inspired by militant religion-based ideologies proliferated across Europe after 2012. Attacks in Australia were far fewer in number, but involved planned beheadings and in 2014 an armed siege of a café in central Sydney with 18 hostages. Alert levels for terrorist attack in Australia or on Australians overseas have remained high for most of the past decade.

Over the decade, another traditional mission of ASD also began to expand: reporting on threats of foreign influence inside Australia. The agency appears to be doing well on that front.

ASIO has been developing its own cyber capabilities but the scale of their efforts is not revealed publicly. Their purpose has been described as 'cyber security monitoring and incident response'.[108]

In the newer missions for ASD (national cyber security policy and practice and an ADF cyber warfare capability) Australia has – not surprisingly – trailed similar reforms in the US by a decade or more. In being responsible for national cyber security outcomes, ASD's own evidence and that of government ministers present a less than satisfactory picture. It will likely need a further decade or more (into the 2030s) to implement these missions at high levels of performance, as long as adequate numbers of trained personnel can be mobilised.

Improvements and additions should be made to the annual ASD Threat Report, especially to bring the full potential of the contributing agencies to bear (AFP, AIC, APRA, ASIO, DFAT, DIO, Home Affairs, OAIC, the Anti-Scam Centre, and the Office of the National Cyber Security

Coordinator). There could usefully be a step-up in the interpretative material provided by some of these agencies to go alongside the excellent ASD data presented. At present, the representation of threats by country (e.g. Russia) in the latest annual threat report is very much a 'bare bones' presentation given that Russia is likely to increase its cyber attacks on Australia.

There is room for some questions about the future.

Does the doubling of investment in new cyber capability, including especially a deepening of domestically oriented surveillance activity, imply a need for significantly enhanced oversight, not to mention more transparency?

In recent years, successive governments have used exaggeration and misstatements of fact to promote in turn an exaggerated sense of threat to Australia, including in cyberspace, while underplaying some other serious threats. Should there be some corrections for the record from the Ministers involved and a return to more balanced analysis and accuracy in statements of policy?

Are the settings for cyber policy and technical education in Australia adequate for all five missions of ASD and their intended scale and intensity? A related question is whether the country should craft a mature policy on reserve options for cyber personnel and operations in the event of war or major confrontation?

---

[1] Australian Signals Directorate, 'Redspice: A blueprint for Growing ASD's Capabilities', 2022, https://www.asd.gov.au/sites/default/files/2022-03/ASD-REDSPICE-Blueprint.pdf.

[2] The paper follows the NATO terminology for cyberspace operations as meaning defence, offence, and intelligence activity. See NATO, 'High Level Taxonomy of Cyberspace Operations', IMSM-0222-2018, June 2018. An important additional aspect in the NATO vision is cyber multi-domain integration, a concept that is central in ADF planning but which receives less attention than it should in public debates.

[3] Australian governments do not consistently make the distinction between previously committed funds and new spending decisions, so this judgement about the increase in the 2024 announcements compared with previous announcements needs to be somewhat qualified.

[4] Department of Defence, 'Targeting threats in the wider frontiers', 26 April 2024, https://www.defence.gov.au/news-events/news/2024-04-26/targeting-threats-wider-frontiers.

[5] See Department of Defence, Portfolio Budget Statements 2023-24, Budget Related Paper No. 1.4a, Defence Portfolio, May 2023, https://www.defence.gov.au/sites/default/files/2023-05/2023-24_defence_pbs_00_complete.pdf; and Department of Defence, 'Budget 2024-25 | Portfolio Budget Statements: Australian Signals Directorate', 2024, https://www.defence.gov.au/sites/default/files/2024-05/2024-25_Defence_PBS_04_Australian_Signals_Directorate.pdf.

[6] See Greg Austin, 'Evaluating Australian Cyber Policy Reform: Urgency, Coherence and Depth', Social Cyber Institute, 2023, https://www.socialcyber.co/_files/ugd/15144d_e47cebbdb5b941ef907c1181488652de.pdf.

[7] Greg Austin, 'Morrison's $1.3 billion for more 'cyber spies' is an incremental response to a radical problem', The Conversation, 30 June 2020, https://theconversation.com/morrisons-1-3-billion-for-more-cyber-spies-is-an-incremental-response-to-a-radical-problem-141692.

[8] Marise Payne, 'Attribution to Russia of malicious cyber activity against Ukraine', 20 February 2022, https://www.foreignminister.gov.au/minister/marise-payne/media-release/attribution-russia-malicious-cyber-activity-against-ukraine. The annual budget of the Australian Signal Directorate in FY2019-20 had previously been set at $763.9 mn, augmented by another $176.8 million for capital investment, for a total of $940.7 million. See ASD, *Annual Report 2019-20*, p. 30. The biggest slice of the $1.35 billion over the decade would be a $470 million investment to increase the cyber security workforce by 500 over a decade, understood to be the civilian employees of ASD. Using this baseline, the government announcement in 2020 of increased spending would have represented an annual budget boost of less than 15% per year on the 2019-20 budget (operations plus special capital injection) and a personnel growth of 25% over the decade.

[9] Department of Defence, 'Budget 2023-24 | Portfolio Budget Statements: Australian Signals Directorate', 2023, p. 64, https://www.defence.gov.au/sites/default/files/2023-05/2023-24_defence_pbs_04_australian_signals_directorate.pdf.

[10] The estimated spend for 2019-20 was $38.3 bn while the budget provision in 2023-24 was $59 bn. See Portfolio Budget Statements 2020-21, Budget Related Paper No. 1.3a, Defence Portfolio, May 2020, p. 17,

https://www.defence.gov.au/sites/default/files/2022-02/2020-21_Defence_PBS_00_Complete.pdf and Portfolio Budget Statements 2023-24, Budget Related Paper No. 1.4a, Defence Portfolio, May 2023, p. 13, https://www.defence.gov.au/sites/default/files/2023-05/2023-24_defence_pbs_00_complete.pdf.

[11] Department of Defence, 'Agency Resources and Planned Performance: Defence Portfolio Budget Statements 2020-21, p. 153, https://www.asd.gov.au/sites/default/files/2022-03/defence_portfolio_budget_statement_australian_signals_directorate_extract_from_defence_2019-20.pdf.

[12] Ibid. p. 124.

[13] Department of Defence, 'Defence Portfolio Budget Statements 2021-22', p. 150, https://www.defence.gov.au/sites/default/files/2022-02/2021-22_Defence_PBS_04_ASD.pdf.

[14] Department of Defence, 'Portfolio Budget Statements | Budget 2022-23', March 2022, p. 151, https://www.asd.gov.au/sites/default/files/2022-04/2022-23_Defence_PBS_04_ASD.pdf.

[15] Department of Defence, 'Budget 2023-24 | Portfolio Budget Statements', p. 164, https://www.asd.gov.au/sites/default/files/2023-10/2023-24%20Defence%20PBS%2004%20ASD.pdf.

[16] Department of Defence, 'Budget 2023-24 | Portfolio Budget Statements: Australian Signals Directorate', 2023, p. 64, https://www.defence.gov.au/sites/default/files/2023-05/2023-24_defence_pbs_04_australian_signals_directorate.pdf.

[17] Department of Defence, 'Budget 2024-25 | Portfolio Budget Statements: Australian Signals Directorate', p. 168.

[18] Ibid.

[19] Ibid.

[20] Ibid.

[21] Ibid.

[22] Australian Signals Directorate, 'Redspice: A blueprint', p. 18.

[23] Ibid. pp. 6-7.

[24] Congressional Research Service, 'Intelligence Community Spending Trends', Updated 26 September 2024, https://sgp.fas.org/crs/intel/R44381.pdf.

[25] Mark Pomerlau, 'US Cyber Command releases first full budget, 13 March 2023, https://defensescoop.com/2023/03/13/us-cyber-command-releases-first-full-budget/.

[26] Australian Signals Directorate, '*Pathways to Engaging with ASD for Capability Delivery*', undated, p. 3, https://www.asd.gov.au/sites/default/files/2023-10/ASD%20Industry%20Brochure.pdf.

[27] US Cyber Command, 'Fiscal Year 2024 Budget Estimates United States Cyber Command', March 2023, p. 4, https://comptroller.defense.gov/Portals/45/Documents/defbudget/fy2024/budget_justification/pdfs/01_Operation_and_Maintenance/O_M_VOL_1_PART_1/CYBERCOM_OP-5.pdf.

[28] Ibid. pp. 8-9.

[29] ASD, 'Annual Report 2022-23', p. 120, https://www.asd.gov.au/about/accountability-governance/publications/asd-annual-report-2022-23.

[30] US Cyber Command, 'Fiscal Year 2024 Budget Estimates United States Cyber Command', pp. 2-3.

[31] This figure included core Cyber Command Staff plus an additional 4,000 personnel assigned from military services and other agencies.

[32] Department of Defence, 'National Defence Strategy', 2024, pp. 29, 38, https://www.defence.gov.au/nds.

[33] Department of Defence, 'Integrated Investment Program', 2024, p. 50, https://www.defence.gov.au/about/strategic-planning/2024-national-defence-strategy-2024-integrated-investment-program. The six areas of capability being pursued are listed on p. 4: (a) project force (b) hold a potential adversary's forces at risk (c) protect ADF forces and supporting critical infrastructure in Australia (d) sustain protracted combat operations (e) maintain persistent situational awareness in our primary area of military interest and (f) achieve decision advantage. All depend on the success of the cyber investments announced in the Integrated Investment Program.

[34] Department of Defence, 'Integrated Investment Program', 2024, p. 50, https://www.defence.gov.au/about/strategic-planning/2024-national-defence-strategy-2024-integrated-investment-program.

[35] Ibid. p. 51.

[36] Department of Defence, 'Ready to Fight and Win in the Digital Age: 2022 Defence Information and Communications Technology Strategy', especially p. 9, https://www.defence.gov.au/about/strategic-planning/2022-defence-information-communications-technology-strategy.

[37] Department of Defence, 'Defence Cyber Security Strategy', https://www.defence.gov.au/sites/default/files/2022-08/defence-cyber-security-strategy.pdf. This was the country's first cyber strategy issued by its Defence Department and focused on network security rather than cyber military strategy in the broad, although there are references to some of those considerations.

[38] Data is drawn from annual reporting by ASD: ASD, 'ASD Annual Report 2018-19', p. 23; https://www.asd.gov.au/about/accountability-governance/publications/asd-annual-report-2018-19; ASD, 'ACSC Annual Cyber Threat Report July 2019 to June 2020', p. 7, https://www.cyber.gov.au/sites/default/files/2023-03/ACSC-Annual-Cyber-Threat-Report-2019-20.pdf; ASD, 'ACSC Annual Cyber Threat Report 2021', p. 19, https://www.cyber.gov.au/sites/default/files/2023-03/ACSC%20Annual%20Cyber%20Threat%20Report%20-

%202020-2021.pdf; ASD, 'ACSC Annual Cyber Threat Report 2022', p. 26, https://www.cyber.gov.au/about-us/view-all-content/reports-and-statistics/acsc-annual-cyber-threat-report-july-2021-june-2022; ASD, 'ASD Annual Cyber Threat Report 2022-23', p 8, https://www.cyber.gov.au/sites/default/files/2023-11/asd-cyber-threat-report-2023.pdf.

[39] ACSC, 'ACSC Annual Cyber Threat Report 2022', p, 12.

[40] Scott Morrison et al, 'Nation's largest ever investment in cyber security', 30 June 2020, https://www.minister.defence.gov.au/media-releases/2020-06-30/nations-largest-ever-investment-cyber-security.

[41] Clare O'Neil, 'Expert Advisory Board appointed as development of new Cyber Security Strategy begins', 8 December 2022, https://minister.homeaffairs.gov.au/ClareONeil/Pages/expert-advisory-board-appointed-as-development.aspx.

[42] '2023-2030 Australian Cyber Security Strategy', pp. 6-7.

[43] Samira Sarraf, 'Australia's new cybersecurity strategy: Build "cyber shields" around the country', CSO, 18 September 2023, https://www.csoonline.com/article/652708/australias-new-cybersecurity-strategy-to-build-6-cyber-shields-around-the-country.html.

[44] Clare O'Neil, Reply to Question without notice, 15/06/2023, Hansard, Parliament of Australia, House of Representatives. https://www.aph.gov.au/Parliamentary_Business/Hansard/Hansard_Display?bid=chamber/hansardr/26705/&sid=0092.

[45] See Paul Karp, 'Peter Dutton confirms plan to create new spying powers still being considered', The Guardian, 16 June 2019, https://www.theguardian.com/australia-news/2019/jun/16/peter-dutton-confirms-plan-to-create-new-spying-powers-still-being-considered; and Paul Karp, 'Peter Dutton confirms Australia could spy on its own citizens under cybersecurity plan', The Guardian , 6 August 2020, https://www.theguardian.com/australia-news/2020/aug/06/peter-dutton-confirms-australia-could-spy-on-its-own-citizens-under-cybersecurity-plan.

[46] See for example Nicola McGarrity and Jessie Blackbourne, 'Australia has enacted 82 anti-terror laws since 2001. But tough laws alone can't eliminate terrorism' 29 September 2019, https://theconversation.com/australia-has-enacted-82-anti-terror-laws-since-2001-but-tough-laws-alone-cant-eliminate-terrorism-123521; and 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.

[47] ASD, 'About', undated, https://www.asd.gov.au/about.

[48] ASD, 'Redspice', pp. 6-7.

[49] Dennis Richardson, 'Comprehensive Review of the Legal Framework of the National Intelligence Community' (Richardson Review), Volume 1 of 4: 'Recommendations and Executive Summary; Foundations and Principles; Control, Coordination and Cooperation', December 2019, p. 89, https://www.ag.gov.au/national-security/publications/report-comprehensive-review-legal-framework-national-intelligence-community.

[50] *Ibid*. p. 378. The 1976 date is a reference to a Royal Commission on the intelligence and security services conclude that year, chaired by Justice Hope.

[51] Ibid., p, 289.

[52] *Ibid*. p. 202.

[53] See Edward Kost, '13 Biggest Data Breaches in Australia [Updated 2024]', Upguard, 6 June 2024, https://www.upguard.com/blog/biggest-data-breaches-australia.

[54] ASIO, 'Case Study: Nest of Spies', undated, https://www.transparency.gov.au/publications/home-affairs/australian-security-intelligence-organisation/australian-security-intelligence-organisation-annual-report-2020-21/part-4%3A-report-on-performance/case-study---nest-of-spies.

[55] Department of Home Affairs, 'PSPF Direction Update – July 2024', 8 July 2024, https://www.protectivesecurity.gov.au/news/pspf-direction-update-july-2024.

[56] The text can be found at https://www.ato.gov.au/law/view/fulldocument?filename=PAC20240024#PAC/20240024/00001.

[57] Richardson, 'Comprehensive review of the legal framework of the national intelligence community'.

[58] An overview of this evolution can be found in several publications by the author: 'Australia Rearmed: Future Needs for Cyber-enabled War', Australian Centre for Cyber Security, Discussion Paper #1, University of New South Wales, January 2016, https://www.socialcyber.co/_files/ugd/15144d_6a1eb662e90e4c96beb5ccfa655cbc6a.pdf?index=true; 'Australia's Response to Advanced Technology Threats: An Agenda for the Next Government', co- authored with Jill Slay, Discussion Paper #3, University of New South Wales, May 2016, https://www.socialcyber.co/_files/ugd/15144d_9e5656980b764585ae5f6032f8de83bc.pdf?index=true; 'Human Capital for Cyber Security: The Australian Case', Australian Centre for Cyber Security, Canberra, ACCS Briefing Paper #2, November 2017, https://www.socialcyber.co/_files/ugd/15144d_4b293373c50a42a89c2f376253643652.pdf?index=true; '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; Greg Austin, 'Cyber revolution' in Australian Defence Force demands

rethink of staff, training and policy**',** The Conversation, 4 July 2017, https://theconversation.com/cyber-revolution-in-australian-defence-force-demands-rethink-of-staff-training-and-policy-80317; UNSW Research Group on Cyber War and Peace, 'Australia Needs Civil Defence against the Cyber Storm', Policy Report, March 2019, co-authored with Gary Waters, https://www.socialcyber.co/_files/ugd/15144d_225b0b0b86b84580b07cbb0c670583f2.pdf; 'Civil Defence Gaps under Cyber Blitzkrieg', Working Paper #6, UNSW Canberra Cyber, February 2019, https://www.socialcyber.co/_files/ugd/15144d_70b23e97258f490cabbedb99326024db.pdf?index=true.

[59] IISS, 'Cyber Capabilities and National Power', 2021, pp. 48-9, https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/cyber-power-report/cyber-capabilities-and-national-power---australia.pdf. The author of the current paper was a major contributor to this 2021 IISS report.

[60] White House, 'Joint Leaders Statement on AUKUS', 15 September 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/09/15/joint-leaders-statement-on-aukus/.

[61] White House, 'Joint Leaders Statement on AUKUS', 15 September 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/09/15/joint-leaders-statement-on-aukus/.

[62] For background on the situation up to 2021, see the chapter on Australia in IISS, 'Cyber Capabilities and National Power: A Net Assessment', 2021, 47-55, https://www.iiss.org/research-paper//2021/06/cyber-capabilities-national-power.

[63] Australian Signals Directorate, 'Redspice: A blueprint for Growing ASD's Capabilities', 2022, https://www.asd.gov.au/sites/default/files/2022-03/ASD-REDSPICE-Blueprint.pdf.

[64] Australian Government, 'National Defence: Defence Strategic Review', 2023, p. 19, https://www.theaustralian.com.au/wp-content/uploads/2023/04/NationalDefence-DefenceStrategicReview.pdf.

[65] Ibid., p, 33.

[66] Ibid., pp. 103-10.

[67] Prime Minister and Cabinet, '2024 Independent Intelligence Review', 23 September 2023, https://www.pmc.gov.au/international-policy-and-national-security/national-security/2024-independent-intelligence-review.

[68] Dennis Richardson, 'Comprehensive review of the legal framework of the national intelligence community',

[69] Leagh Ferris, 'National Security Legislation Amendment (Comprehensive Review and Other Measures No. 3) Bill 2023', Australian Parliament, Bills Digest No. 40, 2024, https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/bd/bd2324a/24bd40.

[70] Australian Government, 'National Defence: Defence Strategic Review', pp. 37, 49.

[71] Ibid., p. 51.

[72] Ibid., p. 64.

[73] Ibid., pp. 82-3.

[74] The UN deliberations culminated in the endorsement by the G-20 of the possible voluntary norms for cyberspace published by a UN expert group in 2015

[75] See Greg Austin, 'Australia', in George Christou, Wilhelm Vosse, Joe Burton and Joachim Koops, *Handbook on Cyber Diplomacy*, Palgrave MacMillan, (forthcoming, 2025).

[76] Marise Payne, 'Attribution to Russia of malicious cyber activity against Ukraine', 20 February 2022, https://www.foreignminister.gov.au/minister/marise-payne/media-release/attribution-russia-malicious-cyber-activity-against-ukraine.

[77] Angus Taylor, 'Australian Government attribution of cyber incident to Russia', Dept of Foreign Affairs and Trade, 17 April 2018, https://www.dfat.gov.au/sites/default/files/australia-attributes-cyber-incident-to-russia.pdf.

[78] Australian Cyber Collaboration Centre, 'Australia joins NATO Cooperative Cyber Defence Centre of Excellence (NATO CCDCOE) Locked Shields for the first time], undated, https://www.cybercollaboration.org.au/news/lockedshields2023.

[79] Richard Marles, Strengthening cyber security in our region', Department of Defence, 27 September 2023, https://www.minister.defence.gov.au/media-releases/2023-09-27/strengthening-cyber-security-our-region.

[80] Australian Signals Directorate et al, 'Guidelines for secure AI System Development', 2023, https://www.cyber.gov.au/sites/default/files/2023-11/guidelines-for-secure-ai-system-development.pdf.

[81] Defence, 'National Defence Strategy', p. 38.

[82] *Ibid*., p. 41.

[83] Australian Government. Defence. 'A new era for the cyber domain', 9 August 2024, https://www.defence.gov.au/news-events/news/2024-08-09/new-era-cyber-domain#:~:text=Cyber%20Command%20sits%20alongside%20Cyberspace,other%20force%20elements%20within%20JCG.

[84] *Ibid*. 'As part of Cyber Command's establishment, the Cyber Force Generation branch has evolved into Cyber Forces Group, a command entity. Joint Cyber Unit, Fleet Cyber Unit, 138 Signal Squadron and 462 Squadron have moved into Cyber Forces Group, along with the 1st Joint Public Affairs Unit. The creation of a Joint Data Network Unit, from its previous operational support task role, is planned for the future.'

[85] This division is 'responsible for the integration, operation, management and security of Defence's global strategic communications capability that enable military operations and support Defence business. ICTOD is also responsible at the strategic level to the Chief of Defence Force and Chief of Joint Operations for advice and technical control for

the Command, Control, Communications and Cyber security in support of ADF Operations.' See Defence, 'Joint Capabilities Group', undated, https://www.defence.gov.au/about/who-we-are/organisation-structure/joint-capabilities-group.

[86] 'The vision of Joint Capability Division is for foundational capabilities for Joint warfighting. The Joint Capability Division mission is to provide timely and effective delivery of integrated capability in order to enable ADF Joint Force interoperability and effects.' See Defence, 'Joint Capabilities Group'.

[87] 'The Military Strategic Effects Branch provides support to the operational and strategic levels through preparation of strategic information activities and strategic targeting support. This enables management of strategic and reputational issues in order for Defence Senior Leaders to appropriately engage with government, other agencies, allies, coalition partners and also the Australian and international communities.' See Defence, 'Joint Capabilities Group'.

[88] Greg Austin, 'Australia's Drums of War', *Survival*, August September, 2021, 229-236.

[89] A good example of the sensationalism can be found in a media article, Peter Hartcher and Matthew Knott, 'Red Alert', Sydney Morning Herald, 7 March 2023, https://www.smh.com.au/politics/federal/red-alert-20230306-p5cpt8.html.

[90] This claim is addressed and debunked in Greg Austin, 'China's Military Buildup: the Biggest Since 1945?', Australian Outlook, 19 February 2024, https://www.internationalaffairs.org.au/australianoutlook/chinas-military-buildup-the-biggest-since-1945/.

[91] Richard Marles, 'Launch of the National Defence Strategy and Integrated Investment Program', National Press Club, 17 April 2024, https://www.minister.defence.gov.au/speeches/2024-04-17/launch-national-defence-strategy-and-integrated-investment-program.

[92] Sebastian Strangio, 'China Demanded Halt to Indonesian Drilling Near Natuna Islands: Report', The Diplomat, 2 December 2021, https://thediplomat.com/2021/12/china-demanded-halt-to-indonesian-drilling-near-natuna-islands-report/.

[93] Dzirhan Mahadzir, 'Joint Chinese, Russian Naval Drills Start in South China Sea', USNI News, 15 July 2024, https://news.usni.org/2024/07/15/joint-chinese-russian-naval-drills-start-in-south-china-sea.

[94] John Dotson, 'An Overview of Chinese Military Activity Near Taiwan in Early August 2022, Part 2: Aviation Activity, and Naval and Ground Force Exercises', 7 September 2022, Global Taiwan Brief, Vol. 7, Issue 18, Global Taiwan Institite, https://globaltaiwan.org/2022/09/an-overview-of-chinese-military-activity-near-taiwan-in-early-august-2022-part-2-aviation-activity-and-naval-and-ground-force-exercises/.

[95] Defence. Defence Strategic Update 2020, p. 14, https://www.defence.gov.au/sites/default/files/2020-11/2020_Defence_Strategic_Update.pdf. 'Previous Defence planning has assumed a ten-year strategic warning time for a major conventional attack against Australia. This is no longer an appropriate basis for defence planning. Coercion, competition and grey-zone activities directly or indirectly targeting Australian interests are occurring now. Growing regional military capabilities, and the speed at which they can be deployed, mean Australia can no longer rely on a timely warning ahead of conflict occurring.'

[96] Defence. 'Defence White Paper 2013', p. 30, https://www.defence.gov.au/sites/default/files/2021-08/WP_2013_web.pdf.

[97] Defence, 'A safer and stronger Australia - Budget 2020-21', Media Release, 6 October 2020, https://www.minister.defence.gov.au/media-releases/2020-10-06/safer-and-stronger-australia-budget-2020-21.

[98] See Austin, **'**Morrison's $1.3 billion for more "cyber spies" is an incremental response to a radical problem**'**.

[99] For a critical perspective on this timeline published in 2022, see Rex Patrick, 'AUKUS submarine 2040 submarine timeline puts Australian submariners' lives at undue risk', 7May 2022, https://parlinfo.aph.gov.au/parlInfo/download/media/pressrel/8565950/upload_binary/8565950.pdf. Patrick, a former submariner, was a Senator in the Australian parliament at the time.

[100] Parliamentary Library, 'The State of Australia's Defence: A Quick Gide', 27 July 2022, https://www.aph.gov.au/About_Parliament/Parliamentary_departments/Parliamentary_Library/pubs/rp/rp2223/Quick_Guides/StateofAustraliasDefence.

[101] See IISS, 'Cyber Capabilities and National Power: A Net Assessment', pp. 48-49.

[102] Daniel Hurst, 'Russian naval vessels on move north of Australia in leadup to G20', The Guardian, 12 November 2014, https://www.theguardian.com/world/2014/nov/12/russian-naval-vessels-on-move-north-of-australia-in-leadup-to-g20.

[103] Secretary Austin said the following: 'We want to see Russia weakened to the degree that it can't do the kinds of things that it has done in invading Ukraine. So it has already lost a lot of military capability, and a lot of its troops, quite frankly. And we want to see them not have the capability to very quickly reproduce that capability.' See Department of Defense, 'Transcript: Secretary of State Antony J. Blinken and Secretary of Defense Lloyd J. Austin III, Remarks to Traveling Press', 25 April 2022, https://www.defense.gov/News/Transcripts/Transcript/Article/3009051/secretary-of-state-antony-j-blinken-and-secretary-of-defense-lloyd-j-austin-iii/.

[104] Greg Austin, 'The UN's indictment of Russia and its long-term consequences', IISS, 10 March 2022, https://www.iiss.org/en/online-analysis/online-analysis/2022/03/the-uns-indictment-of-russia-and-its-long-term-consequences/.
[105] Department of Defence, '$50 million in Australian support for International Fund for Ukraine', 15 February 2024, https://www.minister.defence.gov.au/media-releases/2024-02-15/50-million-australian-support-international-fund-ukraine.
[106] Marcus Hellyer and Ben Stevens, 'The cost of Defence: ASPI defence budget brief 2022–2023', ASPI, 2023, p. 23, https://www.aspi.org.au/report/cost-defence-aspi-defence-budget-brief-2022-2023.
[107] See for example, statements by former Labor foreign ministers, in Bob Carr and Gareth Evans, 'China and the US are playing nice for now but flashpoints remain', The Guardian , 31 January 2024, https://www.theguardian.com/commentisfree/2024/jan/31/china-and-the-us-are-playing-nice-for-now-but-flashpoints-remain-they-must-agree-to-peace.
[108] ASIO, 'Careers with ASIO', 2024, https://www.careers.asio.gov.au/public/jncustomsearch.viewFullSingle?in_organid=12852&in_jnCounter=221300661&in_version=&in_jobDate=All&in_jobType=&in_residency=&in_graphic=&in_param=&in_searchbox=YES&in_recruiter=&in_jobreference=&in_orderby=&in_sessionid=&in_navigation1=&in_summary=S.

SOCIAL CYBER INSTITUTE

The **Social Cyber Institute** (SCI) creates new social science insights to complement technology in the fight for a more secure cyberspace that supports individual, community and national interests on an equitable and rights-based foundation. SCI organises webinars, conference participation, and seminars, and publishes opinion, analysis and research reports and papers. SCI is a non-profit organisation supported by the Social Cyber Group which separately offers advisory and training services in cyber policy. https://socialcyber.co/social-cyber-institute

Director: Professor Glenn Withers (glenn.withers@socialcyber.co)

SOCIAL CYBER ACADEMY

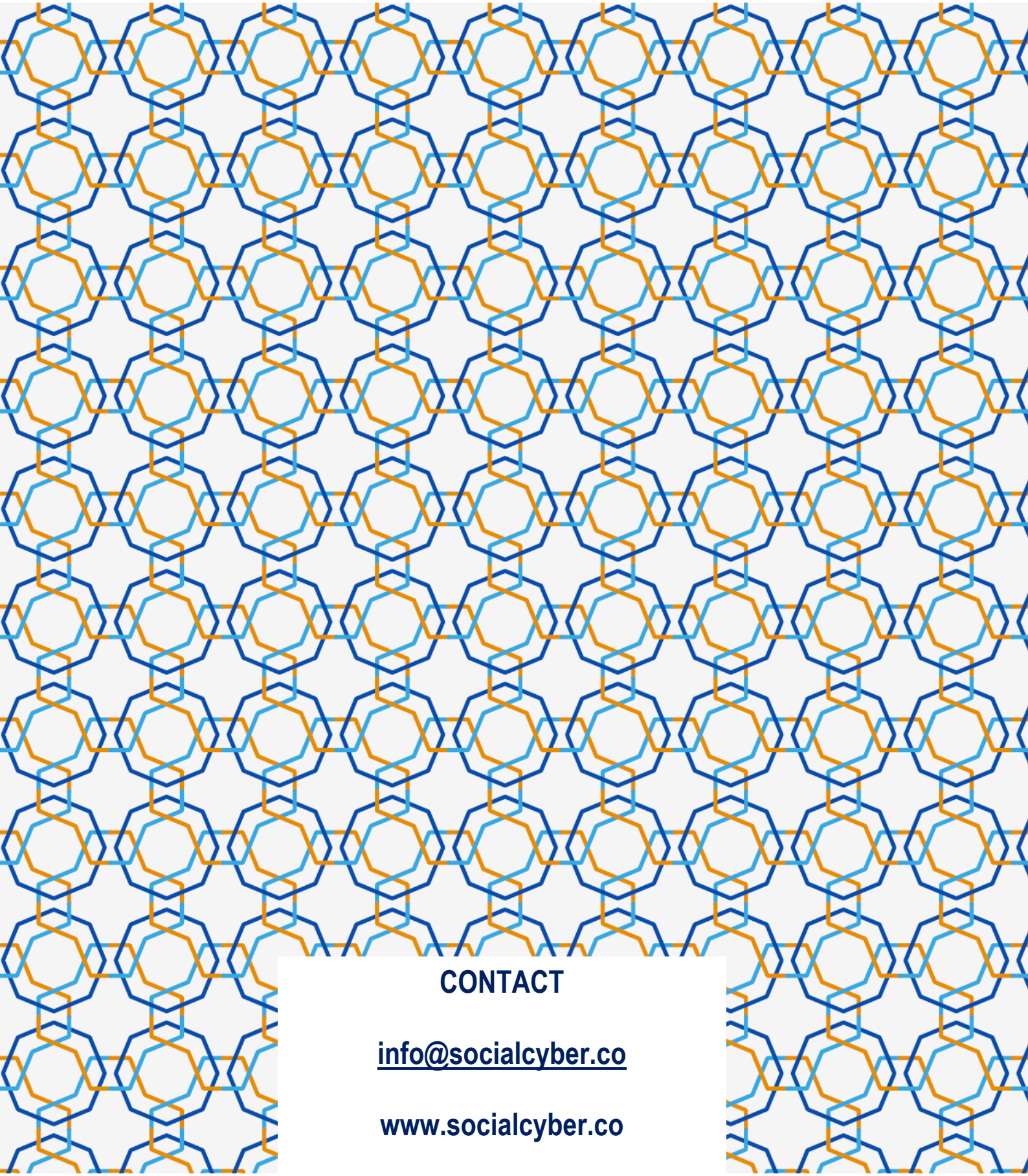
The **Social Cyber Group** (SCG) and **Blended Learning International** (BLI) join forces to deliver exciting international learning experiences with high business and policy relevance, through the Social Cyber Academy. Our dedicated partners in similar professional education activities in recent years have included the **Korea Development Institute** and the **Global Development Learning Network** of the World Bank. The leaders of SCG and BLI rely on decades of experience in university-based and professional education in the US, the UK, Australia and Asia. Other clients of our Academy leaders in the field of education delivery in Australia have ranged from the Australian Department of Defence, Victorian Parliament , and the Australian Indigenous Leadership Council, through to Australian Securities Exchange, Commonwealth Bank, QANTAS Engineering, and the Salvation Army and Soldier On plus, overseas, from the Distance Learning Centre (Sri Lanka), National Organisation of Science Teachers and Educators (Philippines), and Tanri Abeng University (Indonesia), to Tongji University (China), the Singapore Exchange, National Economic Action Council (Malaysia), University of Mauritius, and the Vietnam Cryptographic Agency. https://socialcyber.co/academy

Director: Lisa Materano (lisa.materano@socialcyber.co)

SOCIAL CYBER GROUP ADVISORS

The senior researchers in the **Social Cyber Group** have decades of experience in advising government from inside and outside, often at high levels, and working with business leaders to address their strategic and operational needs. Their clients have included the UK Foreign Office, the UK Ministry of Defence, the UK Cabinet Office, the European Commission, the New South Wales government, the Australian Department of Foreign Affairs and Trade, the Australian Director General of National Intelligence, and the Graduate Research Institute for Policy Studies in Tokyo. https://socialcyber.co/advisory

Director: Professor Greg Austin (greg.austin@socialcyber.co)



CONTACT

info@socialcyber.co

www.socialcyber.co