CYBER SECURITY
COOPERATIVE
RESEARCH
CENTRE

SUBMISSION:

Inquiry into national security risks affecting the Australian higher education and research sector

cybersecuritycrc.org.au

Dear Sir/Madam,

Submission: *Inquiry into national security risks affecting the Australian higher education and research sector*

I am pleased to submit the Cyber Security Cooperative Research Centre's (CSCRC) response to the Parliamentary Joint Committee on Intelligence and Security's *Inquiry into national security risks affecting the Australian higher education and research sector*. We commend the Federal Government for continuing to ensure the integrity of Australia's world-leading education sector, both now and into the future.

About the CSCRC

The CSCRC is dedicated to fostering the next generation of Australian cyber security talent, developing innovative projects to strengthen our nation's cyber security capabilities. We build effective collaborations between industry, government and researchers, creating real-world solutions for pressing cyber-related problems.

By identifying, funding and supporting research projects that build Australia's cyber security capacity, strengthen the cyber security of Australian businesses and address policy and legislative issues across the cyber spectrum, the CSCRC is a key player in the nation's cyber ecosystem. The CSCRC has two research programs: Critical Infrastructure Security and Cyber Security as a Service.

The CSCRC is a public company limited by guarantee and will invest $AU50 million of Australian Commonwealth Government funding and additional Participant funding over seven years to 2025 in research outcomes related to our key impact areas. The CSCRC has 25 Participants including seven Research Providers, eight State and Federal Government Agencies/Departments and 10 Industry/SMEs.

We look forward to answering any queries about this submission and welcome the opportunity to participate in future discussions regarding this very important topic.

Yours Sincerely,

Rachael Falk
CEO, Cyber Security Cooperative Research Centre
ceo@cybersecuritycrc.org.au

Introduction

There is no doubt over the past several decades, Australia's higher education and research sector has been in a state of complacency. Little thought or attention has been given to fostering diversity concerning sources of international funding and international students, which has, in many ways, left higher education and research institutions in a precarious position. This has been highlighted starkly by the COVID-19 pandemic, which has shone a light on the overreliance on international student fees by our universities.

While national security risks stem from a variety of sources, infiltration and interference through the higher education and research sectors has the potential to be especially insidious through its subtlety. Hence, this inquiry is both timely and pertinent, particularly in light of the shifting geopolitical environment.

As noted by the Director-General of Security Mike Burgess in his first annual threat assessment: "The level of threat we face from foreign espionage and interference activities is currently unprecedented. It is higher now, than it was at the height of the Cold War".[1] And the higher education and research sectors are not immune – they are targets. And for many years, they have been soft targets.

The CSCRC is acutely aware of the risks foreign interference presents to our nation's research community and the valuable IP it produces. This IP has the potential to facilitate Australia's progress, both economically and strategically. For this reason, it is also valuable to others.

The CSCRC strongly supports the pursuit of academic freedom and understands that by its very nature, academic collaboration can be undertaken on quite an 'ad hoc' basis. Furthermore, the vast majority of research collaboration is of little consequence to national

[1] https://www.asio.gov.au/publications/speeches-and-statements/director-general-annual-threat-assessment-0.html

security. However, where research does have the potential to leverage Australia's capability and has national security implications, strong protections must be established.

Espionage and foreign interference will remain serious threats to Australia's national security and, while there is no silver bullet solution, risk management and mitigation strategies can help bolster the nation's higher education and research sectors against intrusions.

To this end, the CSCRC has several key recommendations, which we expand upon in this submission:

- Steps must be taken to diversify the contingent of international students studying at Australia's higher education and research institutions, with a focus on the recruitment of students from ally nations;
- The higher education and research sector must diversify the sources of research collaboration and funding being undertaken, with a key focus on fostering stronger partnerships with key allies;
- Cyber security, data protection and IP protection must be of the utmost importance to Australia's higher education and research sector and move beyond just being 'guidelines';
- More stringent oversight and compliance enforcement of the provisions of the *Defence Trade Controls Act 2012*.

Diversification of international student intake

International students bring many social, cultural and economic benefits to Australia. However, the overreliance of Australian universities on full-fee paying international students has been acutely highlighted during the COVID-19 pandemic.

In an ominous warning, a 2019 report by the Centre for Independent Studies (CIS) stated: "As long as their bets on the international student market pay off, the universities' gamble

will look like a success. If their bets go sour, taxpayers may be called on to help pick up the tab".[2]

In 2017-18, international education was worth $32.4 billion to the Australian economy,[3] making it the nation's third largest export. In 2019, Chinese students accounted for the vast majority of international enrolments, representing 37.3 per cent of all higher education enrolments, followed by India, at 20.5 per cent. However, as a result of the pandemic and the subsequent drop in international student numbers, Universities Australia has estimated universities will lose between $3-4.6 billion in 2020, with flow on effects for years to come.[4]

In addition to full fee paying undergraduate international students, universities have also been over-reliant on international students for research and development work. Post-graduate students comprise 57 per cent of the university research and development workforce and 37 per cent of PhD students in Australia are international students, with 75 per cent of those enrolled in science-related degrees.[5]

To justify their growing reliance on full-fee paying international students, universities have cited decreased government funding. However, as highlighted by the CIS, "although Australian universities may use international student fee revenue to offset slight declines in Commonwealth funding, the extraordinary expansion in international student enrolments over the last two decades cannot realistically be attributed to cuts in government funding".[6]

Hence, there is a need to diversify Australia's intake of international students, with a focus on students from nations socially, politically and strategically aligned to ours. This will only

[2] https://www.cis.org.au/app/uploads/2019/08/ap5.pdf , p 1.
[3] https://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/pubs/rp/rp1819/Quick_Guides/OverseasStudents
[4] https://www.universitiesaustralia.edu.au/media-item/investment-in-university-research-an-investment-in-covid-19-recovery/
[5] https://www.science.org.au/sites/default/files/rrif-covid19-research-workforce.pdf, p 2.
[6] https://www.cis.org.au/app/uploads/2019/08/ap5.pdf, p 3.

serve to strengthen Australia's relationships with its key allies and drive mutually beneficial partnerships.

In a recent opinion piece, Peter Jennings and Robert Clark of ASPI wrote that the current climate "presents a significant opportunity for universities that are willing to work with Defence across the Five Eyes countries and take steps to protect their systems and research, particularly when their funding base has been hit hard by COVID-19 impacts … a Five Eyes friendly university sector will open new and substantial sources of funding and help strengthen Australia's defence and security capabilities and of our democratic allies".[7]

Diversification of research collaboration and funding

While the pandemic has undoubtedly wreaked havoc on Australia's higher education and research sector, there has been a silver lining – the realisation research and development can thrive even when researchers are not in the same room or even the same country.

In this regard, there is a momentum that can be harnessed right now to recalibrate research funding and collaborative and strategic relationships. Such a recalibration should prioritise strengthened research collaboration with Australia's strategic allies, including the nations of the Five Eyes and The Quad, with which such partnerships are currently lagging. It makes strategic and economic sense to leverage these relationships for mutually beneficial research outcomes. It is also vital in relation to critical technologies like 5G, the development of which Australia and many of its allies have failed to embrace in a timely manner. Currently, none of the Five Eyes nations has a significant vendor of 5G technologies.[8] Given the importance such technology will have now and into the future, compounded with the potential national security risks 5G presents, this is problematic.

According to a recent report by the Australia-China Relations Institute (ACRI), China has overtaken the United States as Australia's leading research partner, [9] with the proportion of

[7] https://www.aspi.org.au/opinion/university-funding-can-be-boosted-through-defence-research
[8] https://www.techradar.com/au/news/five-eyes-needs-major-5g-vendor
[9] https://www.australiachinarelations.org/content/australia-china-science-boom

Australian scientific publications involving a researcher affiliated with a Chinese institution increasing from 3.1 per cent in 2005 to 16.2 per cent in 2019. Collaboration was most prominent in the areas of materials science, chemical engineering, energy, engineering and physics and astronomy (descriptors of the specific fields each area comprised were not provided).[10]

Promoting industry-led research, like that undertaken at the CSCRC and by the Cooperative Research Centres (CRC) Program more broadly, would also support diversification of research collaboration and funding. By bringing academia, industry and government together, CRCs hone-in on research that responds to real-world and pressing problems, producing research that is both tangible and relevant. This would help alleviate research funding shortfall(s) and protect Australia's international research and innovation. Currently, such enhanced collaborations outside the CRC program are limited because Australia's current level of business research and experimental development is low, compared to the OECD benchmark, sitting at 1.97 per cent of GDP in 2018 as compared with the OECD average of 2.4 per cent.[11] Despite the current shortfall, this is an area of significant opportunity and one that should be explored and promoted by the Federal Government, which could incentivise industry to invest in research and development into the future. While the CSCRC notes the Department of Industry, Science, Energy and Resources does offer a Research and Development Tax Incentive, the threshold for eligibility should be increased to take in companies with turnover of more than $20 million a year.[12]

Cyber security, data protection and IP protection uplift

While ideas are free, protecting them comes at a cost – and intellectual property must be protected vigorously. Hence, cyber security is essential to ensuring Australian-produced IP and data remains safe.

[10] The Australia-China science boom, ACRI, James Laurenceson Michael Zhou, p 8.
[11] https://data.oecd.org/rd/gross-domestic-spending-on-r-d.htm
[12] https://www.industry.gov.au/funding-and-incentives/research-and-development-tax-incentive

If passed, the Federal Government's proposed changes to critical infrastructure legislation, which will capture the education sector, will establish minimum security standards for higher education and research institutions. This will greatly enhance capacity to protect sensitive IP. Furthermore, under the proposed Positive Security Obligation for critical infrastructure providers, organisations will be required to report serious cyber security incidents to the Australian Cyber Security Centre (ACSC). In addition, critical infrastructure entities will be required to develop and comply with a critical infrastructure risk management program and critically address cyber security risks alongside physical, personnel and supply chain risks.[13] The elevation of cyber security threats alongside other well-known risks will ensure education entities' responsivity to an ever-changing threat environment, given their systemic reliance on digital systems. Because at all times the globally interconnected nature of these communication networks remains vulnerable to cyber security threats.

Australian universities are no stranger to malicious cyber activity, with the most high-profile example being the hacking of the ANU in November 2018. The spear-phishing email attack resulted in the breach of the network's Enterprise Systems Domain (ESD), which housed human resources, financial management, student administration and enterprise e-forms systems.[14]

By gaining access to ESD, the actor was able to copy and steal an unknown quantity of data, which covered a period of 19 years. Indications of an intrusion were first detected in April 2019 during a baseline threat hunting exercise, which uncovered network traffic data suggesting the presence of a malicious actor.[15]

The incident response team uncovered the data breach on Friday 17 May and verbally reported it to the Vice-Chancellor that day. The actor's dwell time on the ANU network was

[13] https://www.homeaffairs.gov.au/reports-and-pubs/files/exposure-draft-bill/exposure-draft-security-legislation-amendment-critical-infrastructure-bill-2020-explanatory-document.pdf, p 47.
[14] https://imagedepot.anu.edu.au/scapa/Website/SCAPA190209_Public_report_web_2.pdf
[15] https://imagedepot.anu.edu.au/scapa/Website/SCAPA190209_Public_report_web_2.pdf

approximately six weeks, with most malicious activity ending around mid-December 2018, although there were several further attempts to gain network access.[16]

The CSCRC notes cyber security was a key focus of the University Foreign Interference Taskforce and its *Guidelines to counter foreign interference in the Australian university sector* (the Guidelines).[17] The Guidelines emphasise the need for: implementation of university cyber security strategies; cyber-intelligence sharing across the sector and with government; cyber security as a whole-of-organisation 'human' issue; and cyber threat modelling to understand and mitigate risks.[18] While the CSCRC is highly supportive of these principles it must be stressed that cyber security has to be viewed as more than a compliance issue – it must be seen to be done. To this end, cyber security compliance never stops. Given the rapid pace of technological advancement and increasingly diverse and complex threat vectors, cyber security systems and the data that flows through them must always be front of mind for higher education and research institutions.

The need to protect research IP has been highlighted during the COVID-19 pandemic, with malicious cyber actors around the world trying to access systems in a bid to steal data related to a vaccine. Domestically, the Australian Intelligence and Security Organisation (ASIO), worked with medical and scientific organisations to ensure their research was not stolen.[19] Australia also called out Russia, after the United States, United Kingdom and Canada announced Russian hackers had targeted organisations involved in the development of a COVID-19 vaccine. In July, the United States Department of Justice also accused the Chinese Government of hacking firms developing coronavirus vaccines.[20]

---

[16] https://imagedepot.anu.edu.au/scapa/Website/SCAPA190209_Public_report_web_2.pdf
[17] https://www.dese.gov.au/uncategorised/resources/guidelines-counter-foreign-interference-australian-university-sector
[18] https://www.dese.gov.au/uncategorised/resources/guidelines-counter-foreign-interference-australian-university-sector, p 30.
[19] https://www.abc.net.au/news/2020-08-24/asio-preventing-theft-of-australian-coronavirus-vaccine-research/12584206
[20] https://www.abc.net.au/news/2020-07-22/us-says-chinese-hackers-targeted-coronavirus-vaccines/12479162

In this context, it is also worth mentioning Operation Cloud Hopper, which was one of the largest ever sustained global cyber espionage campaigns. It saw China's cyber espionage group, APT10, target IT managed service providers (MSPs), gaining access to sensitive intellectual property, intelligence and corporate and personal data.[21] It is believed the group was operating in this capacity for approximately 10 years before being uncovered in 2016.[22] Operation Cloud Hopper impacted, among other organisations, NASA and 45 US tech giants, and at least 12 countries, including Australia. The Australian Cyber Security Centre's 2018 investigation report, *Compromise of an Australian company via their Managed Service Provider*, details a computer compromise on the Australian arm of a multinational construction services company via an MSP, which was reported in March 2017.[23] The computer was compromised with specific malware that was previously publicly attributed to APT10.[24] As a result of the breach, which had been initiated in 2016, all corporate user and computer account details, including encrypted passwords were stolen.[25] While the example of Operation Cloud Hopper does not relate directly to the higher education and research sector, it does illustrate how malicious cyber actors can lie in wait, locate and exploit vulnerabilities via third-party providers. This should be of particular concern to the sector, which often relies on third-party providers for essential services.

Oversight and compliance with the provisions of the *Defence Trade Controls Act 2012*

Australia's export control system aims to stop military goods and technology—and goods and technology that can be used in chemical, biological and nuclear weapons—from being transferred to individuals, states or groups with interests prejudicial to Australian interests.[26] As a member of international export control regimes, Australia is part of a

[21] Operation Cloud Hopper | Cyber | Consulting | PwC Australia
[22] Operation Cloud Hopper (pwc.co.uk)
[23] msp_investigation_report.pdf (cyber.gov.au)
[24] msp_investigation_report.pdf (cyber.gov.au)
[25] msp_investigation_report.pdf (cyber.gov.au)
[26] https://www1.defence.gov.au/business-industry/export/controls/export-controls/legislation-regimes-agreements

global effort to regulate the export of items controlled by these regimes, which have military or weapons of mass destruction (WMD) applications.

The 2018 *Independent Review of the Defence Trade Controls Act 2012*[27] flagged there were a number of loopholes in the *Defence Trade Controls Act 2012* (the Act) that might allow for potential vulnerabilities concerning the export of Australian goods and put forth recommendations to bolster the Act's mechanisms. Likewise, the CSCRC advocates for more stringent oversight and compliance enforcement of the provisions of the Act, noting they currently have limitations which need addressing.

While the CSCRC recognises that open collaboration with external organisations is an important element of technology research and accepts the concerns from the research community that the Act could impinge on the sector,[28] this recommendation is made in sober consideration of the changing geopolitical and security environment. Since the 2018 review, the environment has evolved exponentially against the backdrop of a global pandemic and heightened geopolitical tensions.

Greater consideration needs to be given to recent technological advancements and the human capital equation to ensure the Act remains fit for purpose. Furthermore, the provisions should be reviewed and updated on a regular basis. Any subsequent changes should be clearly communicated to all requisite stakeholders including the research community, given that the 2018 Review found there is a need for additional guidance to understand the Act's provisions, given its complexity.

The CSCRC also notes there is scope to tighten exemptions under the Act, where a permit is not required for the supply and publication of dual-use technologies, particularly:

- Exemption for publication: A person does not need approval to publish dual-use Defence and Strategic Goods List (DGSL) technology. However, the Minister for Defence

[27] https://www.defence.gov.au/publications/reviews/tradecontrols/Docs/DTC_Act_Review_Final_Report.pdf
[28] DTC_Act_Review_Final_Report.pdf (defence.gov.au), p 13.

may issue a notice prohibiting publication of certain dual-use DSGL technology, if the publication would prejudice Australia's security, or international obligations.

- Exemption for verbal supply: Verbal supply of DSGL-listed software and technology does not require a permit. This includes telephone conversations, video conferences and live streaming. Face-to-face discussions, either wholly within Australia or wholly outside of Australia, are not regulated and do not require a permit.
- Exemption for basic scientific research: Basic scientific research means: "... experimental or theoretical work undertaken principally to acquire new knowledge of the fundamental principles of phenomena or observable facts, not primarily directed towards a specific practical aim or objective." If your research is applied or experimental developmental it may still be affected by the DTCA.
- Exemption for work in the public domain: In the public domain means: "... technology or software which has been made available without restrictions upon its further dissemination (copyright restrictions do not remove "technology" or "software" from being "in the public domain").

These 'loopholes' are problematic, with the potential to introduce vulnerabilities into the Act's provisions. Noting the changed security and technology environment since the Act's establishment, including sustained activity by foreign actors to conduct technology transfer, these exemptions need revisiting.

Finally, the CSCRC notes there is an opportunity to look to global best practice, most notably the export regime of our key ally, the United States, which has established a strong compliance approach to export controls.[29] This has raised awareness and uplifted the security and integrity of exports. While this approach may not be entirely suitable in the Australian context, there are opportunities to establish a stronger enforcement approach to ensure wider awareness and greater compliance.

[29] https://www.trade.gov/us-export-controls