University of South Australia

SUBMISSION

2023-2030 AUSTRALIAN CYBER SECURITY STRATEGY DISCUSSION PAPER

1. We appreciate the opportunity to make a submission to the Expert Advisory Board discussion paper on the *2023 – 2030 Australia Cyber Security Strategy* and commend the broad multistakeholder consultations to inform the formulation of the strategy.

2. We acknowledge that the ongoing digital transformation means that every aspect of our lives increasingly relies on digital technologies in some way or form, and that any stresses, shocks, and hazards to digital systems impact the wellbeing, safety, and security of the nation. The ensuing cyber-physical-social confluence enabled by digital technologies offers innumerable opportunities for individuals, communities, businesses, government, and society. However, leveraging these opportunities and reaping the associated benefits requires building a whole-of-society cyber resilience and capacity to *prepare for*, *withstand*, *recover*, and *adapt to* the inevitable risks of this digital age.

3. Noting that national cybersecurity strategies are guided by overarching principles that articulate core national values and a vision for a desired cyber future, we are confident that the 2023 – 2030 strategy will clearly articulate such principles and build on those from the 2016 and 2020 cybersecurity strategies, such as:

    a. **Whole-of-society** cyber **resilience**: recognizing that all sectors of society are directly or indirectly dependent on digital technologies and therefore affected by adverse cyber incidents; that it is necessary to ensure continuity of business as usual and life as usual amid and despite the adverse cyber incidents; and that cyber resilience is a systemic attribute that requires strengthening every sector of society. This principle recognizes the need for the strategy to be inclusive and to leave no one behind.
    b. **Transformative partnerships** for **co-production** of cyber resilience: this principle not only recognizes the need for collaboration and cooperation towards national cyber resilience, but also the need for deep partnerships that empower and give agency to the different sectors to meaningfully contribute to creating a cyber resilient society. Partnerships between government and business, as the critical infrastructure owners and the engine of the economy, have traditionally been easier, as has partnerships with formal education entities. However, there is an opportunity, with this strategy, to catalyse quadruple-helix partnerships between government, business, academia, and communities towards national cyber resilience.

4. **Multifaceted and multidimensional cyber space**: cyber space does not only comprise the niche technical domain, but is an assemblage of multiple facets, dimensions, and domains. As result the strategy needs to be comprehensive; for example, it should, at least, be seeking to strengthen each of the five dimensions of the Cybersecurity Capacity Maturity Model for Nations [1], namely *Cybersecurity Policy and Strategy* (D1), *Cybersecurity Culture and Society* (D2), *Building Cybersecurity Knowledge and Capabilities* (D3), *Legal and Regulatory Frameworks* (D4) and *Standards and Technologies* (D5).

5. We observe that to become a world leader in cybersecurity, which is one of the aspirations in the strategy, requires making improvements and addressing the weaknesses identified in key cybersecurity maturity indices. For example, the International Telecommunications Union's (ITU)

Global Cybersecurity Index, noted areas of improvement for Australia on organizational, cooperative, and technical measures.

6. We recognize and appreciate that the strategy has the difficult challenge of remaining relevant for the 2023 to 2030 period (a very long time in the fast-moving technology world) and of anticipating future cybersecurity challenges associated with the ensuing technology advancements. Given that, we highlight a few areas that, in our estimation, are going to have major impact on cybersecurity in the future and that the Expert Advisor Board should keep in consideration:
    a. **Web3 evolution and impacts on cybersecurity**: while Web3 remains a nebulous and loosely defined concept, at its core it is characterized by decentralized governance, distributed architectures and ledger technologies, and interoperable trustless systems. Web3 will have major implications on data ownership and privacy, user identity, compliance and regulation, and law enforcement.
    b. **Artificial intelligence**: much in the same way that software has revolutionized every sector of society, Artificial Intelligence (AI) is anticipated to have a similar wide-scale impact. When AI, with its generative and autonomy capabilities, becomes a critical layer and core fabric of the cyber infrastructure, securing the cyber space will require addressing the concerns associated with adversarial AI and putting in place relevant compliance and accountability mechanisms.
    c. **Complexity of risks**: the global risk landscape is generally very complex; however, recent globalization and digital transformation developments mean that risks cascade quickly not only across sectors but also across countries; COVID19 provided a perfect example of this phenomena. Managing cyber risks necessarily needs to be located within a broader national risk management strategies and plans and within existing regional and international cooperation frameworks. Tools such as complex systems modelling can help map out and operationalize risk management plans in a way that recognizes and accounts for these complex interactions.
    d. **Weaponized interdependence in cyber space**: global information assemblages comprise critical nodes which afford specific countries asymmetric control and leverage towards geostrategic outcomes. Ensuring a sovereign and assured capability to counter cyber threats requires understanding the levels of exposure and dependence on these key control nodes, and employing technical (e.g., redundancy, localization) and diplomacy instruments to address the associated risks.

Below we provide a further response to specific elements of the discussion paper:

Core policy areas

7. Enhancing and harmonizing regulatory frameworks

a. There is an opportunity not only to align and harmonize, but also to delineate, the national cybersecurity strategy with respect to several other related regulatory frameworks. Of relevance are the National Strategy for Disaster Resilience (NSDR), the Critical Infrastructure Resilience Strategy, and the International Cyber and Critical Technology Engagement Strategy.

b. While primarily formulated with emphasis on natural risks and disasters, the National Strategy for Disaster Resilience provides a strong whole-of-society and resilience-based approach that can inform and encapsulate the framing of the national cybersecurity strategy. Worth noting from this strategy is the operationalized acknowledgement that "disaster resilience is a shared responsibility between governments, communities, businesses and individuals" and intention of the strategy to provide actionable guidance to all

sectors of society towards resilience [2].

We recommend that, in consideration of this broad national framing of dealing with disasters, which cyber threats can evolve into, the national cybersecurity strategy should similarly and primarily be framed to recognize the need for deep partnerships and to clearly articulate the roles and responsibilities of every sector of society, along with government and CI owners, towards whole-of-society cyber resilience.

c. Understandably critical infrastructure (CI) and systems of national significance (SoNS) provide a key layer of the cyber space that warrants particular attention to ensure broader societal cyber resilience. However, the cyber space is much more than the critical infrastructure. Recognizing that several CI instruments and legislative frameworks, such as Critical Infrastructure Resilience Strategy, Critical Infrastructure Resilience Plan, Security of Critical Infrastructure Act, and Security Legislation Amendment Critical Infrastructure Protection Act, are already in place, we see this as an opportunity for the national cybersecurity strategy, while aligning with and referencing these CI instruments, to provide further impetus and guidance to other sectors of society (e.g., civil society, SMEs) that have traditionally been marginalized in cybersecurity.

d. There is an obvious need for a strong alignment between the National Cybersecurity Strategy and the International Cyber and Critical Technology Engagement Strategy. We note, with interest, that the latter provides a much more comprehensive guide and elaborate plan of action on critical issues that are not only of international but also domestic interest; for example – cybercrime, online harms and safety, markets and supply chains, internet governance, disinformation, and misinformation. We understand that some of these issues might be classified more under online safety than cybersecurity, however, as aspects of the safety and security of the domestic cyber space, we recommend that the strategy provides guidance of these issues or reference the International Cyber and Critical Technology Engagement Strategy.

8. Strengthening Australia's international strategy on cyber security

a. We recognize that the International Cyber and Critical Technology Engagement Strategy does a great job of providing a very comprehensive primary guidance on international engagement on cyber issues.

b. Australia's engagement in the different United Nations processes, including the UN Group of Governmental Experts (UN-GGE) and in the Open-ended Working Group on the security of and in the use of information and communication technologies (UN-OEWG) are commendable and remain the critical mechanisms for shaping the greatly contested global cyber order. Strengthening and building partnerships with intergovernmental organizations, including UN entities such as UN Women on gender and cybersecurity, UNODC on cybercrime, and UNIDIR on implication of cyber on international security, will help elevate Australia's engagement and leadership in the international arena.

c. There are great opportunities for the government to partner with multinational industry entities, including critical infrastructure owners, not only towards strengthening domestic cyber security goals but also toward enhancing regional and international cyber resilience. These partnerships will provide an opportunity to share best practices across countries and jurisdictions, to harmonize international cybersecurity frameworks and standards (e.g., ISO/IEC 27110:2021 and ISO/IEC 27103: 2018) across the region, and to facilitate cooperation and interoperability for incident response.

Potential policy areas

9. Supporting Australia's cyber workforce and skills pipeline

a. We observe that the global cybersecurity skills gap has continued to rise in recent years, estimated at 2.72 in 2021 and 3.4 million in 2022 [3]. The global competition for cybersecurity professionals puts pressure on Australia not only to attract international talent but also to retain local talent.

b. Addressing this challenge requires a recognition that it is not only about the headline supply and demand gap, but also about technical versus soft skills gap, diversity gaps, and sectoral gaps [4]. As such, while the STEM disciplines are an important element of the overall cyber capabilities mix, it would be limiting and short-sighted to predicate the national cyber workforce on the STEM skills pipeline alone. The 2022 $(ISC)^2$ workforce study found that while most cybersecurity professionals had Bachelor's and Master's degrees in Computer Science, IT and Engineering fields, 30% had training in other disciplines; this number rises to 40% for those with Doctorate degrees and 45% for Post-doctoral studies [3]. We recommend that the strategy outlines complementary skills pipelines that will feed into non-technical cybersecurity career pathways such as policymaking, governance, risks, and compliance; social and cultural engineers; psychologists; and cyber diplomacy.

c. We recognize that there is a vast continuum of skills competencies from basic cyber hygiene to high-end professional cybersecurity skills which are all needed to advance national cyber resilience. As such, we see opportunities for greater harmonization and complementarity between various digital and cyber capacity development instruments such as the Department of Education's National STEM School Education Strategy [5], the Department of Education, Skills and Employment's Digital Literacy Skills Framework [6], and professional certification programs.

What more can the Australian Government do to support Australia's cyber security workforce through education, immigration, and accreditation?

d. There needs to be more focused attention afforded to critical infrastructure protection. The government invested in a significant uplift to SOCI and there will be ongoing requirements to enforce, assess, and respond to major incidents against Systems of National Significance (SoNS) or other organisations in the new critical infrastructure sectors. Many critical infrastructure assets depend on Operational Technologies (OT) such a Programmable Logic Controllers (PLC), Supervisory Control and Data Acquisition (SCADA), Industrial Control Systems (ICS), and even the Industrial Internet of Things (IIoT). These systems are highly bespoke and cannot be secured using standard IT cybersecurity knowledge and frameworks. The government needs to support the development of OT security skills and cyber security frameworks.

e. IT, computer science and engineering education continue to play a crucial role in cyber security. However, there remains ample room for engineering education in Australia to be infused with cyber security elements. In fact, Cyber Engineering, as spearheaded by Prof Jill Slay AM and Engineers Australia, is meant to capture this infusion: Cyber Engineering involves the design, implementation, maintenance, and improvement of measures used to protect the confidentiality, integrity and availability of systems and information. Engineers Australia already has a Cyber Engineering Community of Practice, and University of South Australia for example has a Master of

Cyber Engineering and Telecommunications program, but Cyber Engineering has yet to penetrate engineering education in general. Influencing engineering accreditation bodies, such as Engineers Australia, to mandate crucial cyber security elements in engineering education – in the name of Cyber Engineering or not – is an important way the Government can support Australia's cyber security workforce.

10. National Frameworks to respond to major cyber incidents

a. We note that major cybersecurity incidents can have an impact equitable to national (natural) disasters and therefore see a potential for cyber incident response to align with the whole-of-society, multi-level coordination and response framing that is defined in the National Strategy for Disaster Resilience.

How should the Government respond to major cyber incidents (beyond existing law enforcement and operational responses) to protect Australians?

b. The strategy should discuss capabilities and modalities for the government to respond to national incidents. For example, after Optus and Medibank cyber-attacks, an announcement for offensive response to large cyber-attacks was made. The strategy should provide clarity on how such capabilities and interventions would be managed and deployed.

11. Community awareness and victim support

a. Globally SME and civil society stakeholder (e.g., NGOs, CSOs, CBOs) remain marginalized in cybersecurity, representing a major handicap to whole-of-society cyber resilience. Australia will only be as cyber resilient as its least resilient sector. The strategy should give attention to strengthening the cyber resilience of these marginalized stakeholders. Further, sector focused CIRTs should be established and supported to provide incident response to "non-critical" sectors.

b. We note that the previous strategy (2020) recognized the responsibilities of community stakeholder, however these are largely framed as beneficiaries of cybersecurity measures (e.g., under the themes such as "access and apply guidance and information on cyber security", "make informed purchasing decision", "access help and support where needed"). It is important for the strategy to spell out mechanisms and avenues for engagement of community stakeholders in the co-production of cyber resilience; for example, for training and capacity-building for marginalized population groups, intelligence sharing, first response, and recovery interventions for socio-technical cyber threats.

The 2016 national cybersecurity strategy advanced the notion of "A cyber smart nation" which provides an important focus on human-centric cybersecurity and on elevating the human-factors in cybersecurity, which according to many threat intelligence reports, remain the key weaknesses and vectors that are most exploited in cyber-attacks. We recommend that a similar human-centric focus (or objective) be articulated in the strategy to give recognition to the overall goal of the strategy to create a safe, trusted, and secure environment for Australians.

12. Designing and sustaining security in new technologies

How should the Strategy evolve to address the cyber security of emerging technologies and promote security-by-design in new technologies?

a. As stated in the cyber security strategy discussion paper, there are several new and emerging technologies that impact the existing and near future Australian cyber security landscape. The growing interconnectivity of everything, from household devices to critical infrastructure assets and government services, makes the defensible attack surface increasingly difficult to measure and defend. Security-by-design is the only effective countermeasure to this effect but is by its very nature application-specific. This can make cyber security advice or regulatory enforcement ineffective without sector-specific tailoring. Nation-wide this can be assured through the government sponsorship, endorsement, and enforcement of sector-specific security standards (such as the AESCSF for the energy sector).

b. National strategies that reflect emphasis on "security by design" do already exist, for example, the Communications Technologies and Services Roadmap 2021-2030, as part of the Australian Civil Space Strategy 2019-2028, has highlighted cyber security as one of six key cross-cutting technology areas. However, actual developments in the industry often depart from the envisioned roadmaps. It is unclear, for example, how much of the current investment in the Australian New Space sector is directly contributing to "security by design". Ensuring adequate investment in "security by design" is an important way the Strategy should evolve.

   The National Institute of Standards and Technology (NIST) in the U.S. regularly publishes and updates recommendations and frameworks on the cyber security aspects of various technologies, e.g., the recent Artificial Intelligence Risk Management Framework (AI RMF 1.0, NIST AI 100-1). Working closely with the NIST in their effort to update these industry-standard publications is another way the Strategy can evolve.

Once again, we welcome the opportunity to contribute to the shaping of the *2023 – 2030 Australian Cybersecurity Strategy*, and commit ourselves to continuing to partner with government, business, academia, and community to advance our collective cyber resilience.

Professor Marnie Hughes-Warrington AO
Deputy Vice Chancellor: Research and Enterprise
University of South Australia
14 April 2023

References:

[1] Global Cyber Security Capacity Centre, 'Cyber Capacity Maturity Model for Nations (CMM)', 2021. Accessed: Mar. 27, 2023. [Online]. Available: https://gcscc.ox.ac.uk/the-cmm
[2] Commonwealth of Australia, 'National Strategy for Disaster Resilience - Building the resilience of our nation to disasters', Feb. 2011.
[3] International Information System Security Certification Consortium, '(ISC)2 Cybersecurity Workforce Study 2022', 2022. Accessed: Mar. 28, 2023. [Online]. Available: https://www.isc2.org/-/media/2A313135414E400FA0DBD364FD74961F.ashx
[4] M. Thinyane, D. Christine, and K. Detros, 'Here's how to address the workforce gaps in cybersecurity', *World Economic Forum*, Oct. 21, 2022. Accessed: Mar. 28, 2023. [Online]. Available: https://www.weforum.org/agenda/2022/10/cybersecurity-workforce-gaps-inclusive-approach-jobs/
[5] Education Council, 'National STEM School Education Strategy', Text, 2015. Accessed: Mar. 28, 2023. [Online]. Available: https://www.education.gov.au/education-ministers-meeting/resources/national-stem-school-education-strategy
[6] Department of Education, Skills, and Employment, 'Digital Literacy Skills Framework', Text, 2020. Accessed: Mar. 28, 2023. [Online]. Available: https://www.dewr.gov.au/foundation-skills-your-future-program/resources/digital-literacy-skills-framework

Authors: Mamello Thinyane, Jordan Plotnek and Yee Wei Law