Submission Input

Australian Government Department of Foreign Affairs and Trade (DFAT): Cyber and Critical Technology International Engagement Strategy (CCTIES)

15 June 2020

We, the Authors, wish to thank DFAT for the opportunity to provide consideration to the 2020 International Cyber Engagement Strategy (CCTIES).

We retain ownership in the views expressed herein and agree that this submission may be used by the Commonwealth of Australia for Commonwealth purposes and is therefore classified PUBLIC. The views expressed in this submission represent the views of the Authors as individuals, and do not reflect the views of the organisations mentioned in the author introductions, the Commonwealth of Australia, the Australian Government or Australian Government Agencies.

The Authors

Dr Leif Hanlen B.Sc. B.Eng., PhD

Leif is fascinated with combinations of innovation, technology, strategy and data. He has deep experience in developing new Reg-Tech and data-driven products with a background supporting Government and large enterprises adopt such technologies. He was a co-founder of the Regulation Technology platform 'PaidRight' and was previously Technology Director and New Industries Lead for CSIRO's Data61, and eHealth Business Director for National ICT Australia (NICTA). He supported the international standard for wireless Body Area Networks, developed Dark Web analytics for Immigration and led the development of Legislation-as-Data projects.

He is an adjunct Professor of Health at the University of Canberra, adjunct Associate Professor of ICT at the Australian National University. Leif is also a European Union-invited keynote speaker on Reg Tech, and a regular international technology reviewer for the Science Foundation of Ireland.

Leif is currently Executive Director at Synergy Group, where he leads Strategic Data for Australian Government Agencies.

Contact details
Email: leif.hanlen@gmail.com
Canberra ACT

Ms Daniella Traino GAICD, CISM, CISA, CRISC, CA

Daniella focuses on strategic cyber security services (interim Chief Information Security Officer) and high-tech commercialisation for financial services and emerging industries (Fintech, Cyber Security, Industry 4.0). Formerly a Chief Information Security Officer (CISO) for several industries, and Director & Business Leader (Cyber Security) with CSIRO's Data61 where she co-developed the cyber security business strategy for R&D commercialisation. Daniella is a judge for Fintech Australia in several categories and has regularly contributed and published articles in cyber security strategy and innovation. In 2019, she was nominated for the Security Champion award (AWSN & CSO IDG Women in Security Awards) and was a member of the multi-award winning National and State iAwards team (cyber product innovation).

- Managing Director, Pinecone Technology Strategies (http://www.pineconestrategies.tech)
- Member, Research Advisory Council, Internet Commerce Security Laboratory (ICSL Cybercrime Lab), Federation University (https://federation.edu.au/icsl)
- Startup Editor (AI, Cyber Security), IdeaSpies (http://www.ideaspies.com)
- Cyber Track Leader, Spark Festival (www.sparkfestival.co)

Contact details
Email: daniella@pineconestrategies.tech
Sydney NSW

A unique and difficult opportunity

Why a critical market failure?

Cyberspace has several structural features that contribute to market failures in economics and international policy:

- pervasive information asymmetry.
- the industrialisation of learning through artificial intelligence (AI).
- winner-takes-most economics, which results in the proliferation of "superstar" firms or de facto oligopolies and monopolies.
- new forms of trade and exchange in data, the value of which is not captured by traditional economic accounting systems; and
- systemic risks due to vulnerable information infrastructure.

Data-driven and cyber space industries are naturally monopolistic: where a small number of international interests dominate local domestic approaches. The many layers of asymmetry inherent to the data-driven economy – between human and machine intelligence, between firms, and between nations across the digital divide -- call into question a laissez-faire approach to national regulation and economic strategy in the digital age [Ciuriak 2018]. These critical market failures hold Australia back.

Additionally, due to these failures we see Industry globally is increasingly collaborating[1] to share intelligence, knowledge of defensive and preventative techniques and more - there is simply a gap in our arsenal without doing so and cyber security while a competitive advantage, is also foundational/ essential to any and all industries. As cyber threat actors have shown - they already collaborate better and more effectively than our Agencies and Governments.

Current research indicates that critical cyber security skills remain in short supply - 62% of respondents in a recent ISACA global survey (State of Cybersecurity 2020) struggled with understaffing, and those with 'appropriately staffed' cybersecurity teams had a 50% confidence level in their organisation's ability to respond to cyber threats. Domestically & globally these human resource limitations not only lead to future challenges for defenders and resilience, but also present opportunities to rethink the cyber security paradigms and toolkits to prevent, defend and deter malicious activity across our economy and society.

Australia must correct a critical market failure[1] in its cyber security services and capability. We see opportunities, as part of a larger nationally coordinated effort as a good global citizen, to actively create new jobs, and new sources of prosperity for Australia. Our key observation is that DFAT is uniquely placed to provide leadership, and horizon scanning for Australian cyber security objectives with a strong lens on global partnerships, trade, and geopolitical challenges.

There is a path to move from our current state to one which supports a rapid, responsive and resilient digital economy and society. Embracing and measuring clear objectives, investment portfolios (including strategic procurement by Government), and high expectations for Australia within an interconnected and global environment.

Australia has a proud history of making timely shifts in economic investment. Other nations with similar economies have already moved toward active cyber strategies[2]. We now have the opportunity to learn from them and leapfrog international better practice before these other emergent digital economies grow to incumbency. This opportunity is more pronounced as the United States and other great powers are experiencing acute geopolitical and domestic challenges.

[1] Smith, Ingram "Organising cyber security in Australia and beyond" May 2017

[2] In the US, UK, Singapore and India for example, where the Government has taken an active-investor role in emerging technology and research & development, so they can access breakthrough capability for Government services, policy and other nation-building purposes. Refer to the Case studies in our submission paper.

Australia has the opportunity, through cyber security diplomacy to engage more broadly, and more effectively than ever before.

Cyber, digital and data are core components of our living standards. They will not diminish with time. This is more than digital shopping and web-surfing. Cyber technology is essential to our economy: we cannot thrive without strong engagement and participation in a full cyber embedded economy. Without effective cyber security, our society will have a substantially lower economic capability and we risk exacerbating longstanding power imbalances.

We are rapidly moving beyond a "cyber" economy: cyberspace and its outcomes are pervasive throughout (and intrinsic to) the Australian economy such that it is taken for granted. Due to this intrinsic role, any such weakness can be felt across multiple sectors, not just the technological ones, since every sector is becoming (or will become) technology driven.

DFAT should consider at least three aspects to a global cyber security engagement role:

1. Cyber capability as a strategic platform[3] to support Australia's international and domestic objectives.
2. Cyber innovation as a driver, determinant and cadence of change; and
3. Cyber policy as industrial policy, supporting this strategic platform and guiding or aligning the innovation.

Australian principles as a society directly translate and carry over into cyberspace, including values such as the rule-of-law, equality of opportunity and human rights. Although the speed and scale of cyberspace may be much larger than we are used to, our core objectives and values ought to remain unchanged. However, the advent of highly connected, long-term stored and highly accessible information as the new currency, demands clarification and a new emphasis on what we value in our principles. DFAT must therefore use its position to rebuild trust, enhance transparency, reduce the likelihood and impact of malicious activity in cyberspace, establish agreed international cyber & privacy norms & facilitate management for violation of agreed norms.

Cybersecurity should be seen as an investment not a cost. In addition to economic prosperity, other outcomes of value include trust. In these distrustful times, where data integrity is a work in progress and society seems dominated by division and fear, cyber security and privacy help elevate economic and social engagement based on reliable information. DFAT's updated cyber engagement strategy can assist in reaffirming good culture and behaviour, at home and abroad.

[3] Platform in cyber space is a 'double-sided' market mechanism where the users and sellers of product(s) contribute to the service offerings of the platform, however, the platform provides a connection between product buyers and sellers equivalent to a marketplace. Moreover, the owner of the platform tends to dominate the relevant digital market. Google and Amazon are examples of platforms. We adopt a similar concept for a 'cyber platform' which would connect cyber technology users to vendors.

2030 Future State. How will cyberspace and critical technology shape the international strategic/geopolitical environment out to 2030?

Insights:

- People and 'things' create data 'crumbs' and our digital footprint will depend upon how we interact and consume, products and services that we don't necessarily build, operate and regulate in Australia. Cyber diplomacy is therefore critical, with alignment to Australian values, tax and legal frameworks.
- The cost of cloud compute[4] (for example AWS, Google, Azure) is halved every three years, simultaneously, the compute capacity of a given instance (at a fixed price) quadruples every 3 years. The volume of generated data from computational systems doubles every 6 months. The value of a data network grows with the square of the number of participants. **This combined exponential growth means the potential market for a data business doubles every 3 months.**
- Artificial Intelligence (AI) is likely to be near- or beyond the Turing test and hence indistinguishable from human conversation online. AI will be delivered 'as a cloud service' at scale to industry. The basic commodity analytics tools in use by industry could have abilities that are currently limited to the likes of Google research or IBM.
- Potential growth in quantum Machine Learning and AI may drive analytics to faster capacity.
- Technology companies dominate and leverage diversity and data volumes - Google demonstrated the use of data capture in its growth from advertising revenue to major caches of the world's analytics. Microsoft is offering new 'analytics' approaches which are pushing out competition from the wider AI vendor community.
- A winner-takes-most economic approach[5], scaled by 6 orders of magnitude means that major digital corporations and platform providers will be more successful and dominate different regional networks, and more likely to flout or ignore regulation[6] and/or influence government policy.
- Cryptography and privacy growing in a three-way arm wrestle between private citizens and companies looking for protections on their data; law enforcement seeking access to data; and industry offering solutions to both sides. Cryptography, privacy-enabled and cyber-security 'as a service' will become ubiquitous.
- **Trust in a diminishingly trustworthy world.** Advanced malicious cyber activity against Australia's national and economic interests is increasing in frequency, scale, sophistication and severity. Together with the availability of tools-of-the-trade, the more advanced adversaries continue to invest in their capabilities. Staying ahead of these

[4] https://appdevelopermagazine.com/why-the-cost-of-cloud-computing-is-dropping-dramatically
[5] Google vs any other search engine; Facebook vs most other messaging services
[6] Uber, for example, had enough social influence worldwide, and enough commercial backing from Amazon to wait for national regulations to eventually accommodate its business model, rather than complying. Additionally, the December 2018 scenario analysis report (a collaboration between the Sydney Cyber Security Network and ASPI's International Cyber Policy Centre) hypothesises a 2024 future with further scenarios to a fragmentation of the Internet - https://www.aspi.org.au/report/australias-cybersecurity-futures

threats remains an enduring challenge. The focus for most businesses, and the Government should be cyber resilience and data integrity/ provenance.

    - Privacy, cryptography and the use of digital ledgers will grow, in order to allow some parts of the economy to reduce transparency
    - The application of rule of law will tend toward computational approaches (away from manual), and data, with a consequent risk of programmatic bias and (lack of) transparency.
    - Although the share of personal data that the Australian government holds will reduce compared to private industry (e.g. health records vs Facebook posts), the quality assurance and value associated with these rare and private stores will grow: Government will face a data assurance gap.
    - As computational law (AI supported legal approaches) grows, government regulators will find they are outpaced, outgunned and out-spent by the organisations that require most regulatory attention. Although some Australian regulators have sought to address this imbalance, medium-cost AI services will naturally advantage those organisations willing to spend their way out of compliance (both in skills and technology acquisition).
    - Similarly, lower cost, poorer quality approaches are appearing which are inherently vulnerable to attack[7] in addition to new technologies with inherent weaknesses. A segment of the population and businesses of Australia will likely be at risk due to choices of lower-priced equipment and 'consumables'. It is likely that Australian Government standards will be required, which are the cyber equivalent of requiring all cars to have seatbelts and safety features. It will not be acceptable to simply declare 'caveat emptor' for all digital purchases as is the current state.

- The digital supply chain will be critical to the effective operation of the economy. These will require regulators to impose clear (and possibly expensive) requirements. In some cases, this may require intense local development.
    - This may mean the development of key supply chain components locally. This will also require the development of local digitally automated assurance approaches which can certify suppliers and products deemed critical to the economic supply chain.

Predicting technological outcomes is always fraught. However, key trends suggest technology capabilities and a level of concentration of those capabilities:

- **The pace of change is beyond experience-based strategic thinking:** For DFAT **-** how do policy and engagement strategies stay relevant in a blizzard of change?
- **Information asymmetries:** the data that supports 'evidence-based' decisions may be meaningless to human viewers, while the Artificial Intelligence (AI) and decision

[7] Many commodity WIFI routers are still supplied with easily guessed 'default' administrator passwords. The Internet of Things (IoT) shows this inherent vulnerability at scale - with over a million connected 'things' and growing.

processes are inscrutable. How do we trust the outcome? How does DFAT navigate trust?

- **Uncertain and unknown suppliers within our economic shed:** the critical infrastructure upon which businesses operate is built on and with many components of hardware and software, which is unassured or for which assurance is increasingly complex to determine. State-based and state-sponsored cyber espionage increasingly targets civil society and corporations, while attribution is not clear (weaponisation of data makes this increasingly difficult). Supply chain integrity - How do we secure our economy and economic collaborators while connected?
    - A redesigned and re-invigorated manufacturing sector which is oriented to cyber (& related) products and component-based-value manufacturing -- “a things of the internet” and moving beyond physical manufacturing. This supports a more resilient economy that is not significantly impacted by major economic shocks - such as COVID-19, which are likely to become more common before they are overcome.
    - Smart manufacturers of critical and valuable (unique) elements of the supply chain.
- **Winner-takes-most:** the commercial holders of data (not algorithms) and the cyber-incumbents are behemoths whose revenue makes Australian GDP appear trivial. DFAT will need to work even harder to influence global and regional policy, tax and legislative frameworks to uphold Australian interests and values.
- **Workforce transition:** by 2030, Australia is expected to be trending toward 40 million people: over 30% born overseas, those born after 2000 the dominant members of the workforce, with 50% tertiary educated.
    - These are digitally native Australians and highly likely to be cyberspace manufacturers. Global employment has shifted with the growth and prosperity of cyber economies. Does Australia grow this cyber workforce, do we outsource it to our educated neighbours, or do we become the educators/ education platform for our region?

Supply chains: vulnerability and opportunity

Key questions to assess:

- Can we strike a balance between security approaches and (digital) industry services?
- Is there a mechanism to avoid investments that reduce our security?
- How do we avoid a cyber security approach that adversely limits Australian industry?

Software and cyber supply chains (like commodity and manufacturing supply chains) exhibit weakness in product, and also in the skills of those developing the product. Unlike other commodities, cyber products have significant information asymmetry: a weakness or missing element in the supply of a given product may not be known to both buyers and sellers, and current approaches, built on trusted suppliers, and unverified processes mean the underlying root weaknesses cannot be easily determined or prevented. Worse, the use of broadly adopted (unverifiable) software services and products mean that economies of 'smart' systems must rely on trusting unknown and potentially malicious or negligent suppliers and components.

The pace of change in cyberspace and associated technology drives a multi-speed decision process. Technological change occurs on very short (days-to-weeks) cycles and tends to be private and hence invisible prior to public announcement or outcome. This means that strategies built upon best available evidence can become 'out of date' rapidly or derailed during a crisis.

As the COVID19 pandemic brought to bear more clearly and the increasing cases of software supply chain attacks demonstrate[8,9], our reliance on specific countries and a 'trusted but not verified' supply chain have left significant vulnerabilities. Cyber threat actors move and adapt quickly to exploit our society and economic challenges with new tools, techniques and practices at a speed our defenders in industry and government do not consistently match. We must do better to identify these global threats and increase the resiliency of our industries, and build capability to respond, defend and protect Australian values and businesses.

DFAT's cyber diplomacy is one avenue to strengthen the trust and collaboration required. A trusted & validated supply chain - a hybrid of sovereign capability and assured capability -- must be our strategic intent. Trust will be the new competitive differentiator and foundational to our "new normal.". Legislation and regulation supporting secure-by-design and default, privacy-by-design and default should be the non-functional requirement for future industries (smart manufacturing, etc)

[8] https://www.smh.com.au/technology/drinks-giant-lion-hit-by-cyber-attack-as-hackers-target-corporate-australia-20200609-p550pu.html
[9] https://www.cyber.gov.au/threats/summary-of-tradecraft-trends-for-2019-20-tactics-techniques-and-procedures-used-to-target-australian-networks

DFAT should seek an engagement strategy that works with international organisations and consortiums such as for example, FIRST[10] and the World Economic Forum Global Centre for Cybersecurity - to help reduce the global attack surface (less of a defensive position, but more protective/ proactive), build future skills in cyber security & privacy so that Australia has the capability to assure complex solutions for our context.

Australia should focus on smart, domestic manufacturing. The COVID19 pandemic highlighted the global economy's reliance on specific countries and manufacturing capabilities, which raised significant risks. Geopolitical tensions and the cyber security threat environment heighten that risk further. But rather than assume a sovereign capability requires Australia to manufacture everything, we have an opportunity to focus on niche, value-adding components to support global applications - for example, in Quantum Computing our innovators such as Quintessence Labs[11], Q-TRL[12] and Silicon Quantum Computing[13] are leading the world in quantum-secure encryption & key management, quantum control engineering solutions, design and build of a qubit quantum processor. These solutions will power future industry-wide applications.

The global supply chain challenges will only deepen, so what Australia decides to manufacture indigenously and how Australia behaves as a sophisticated buyer will be key. The point is that these strategies for national and supply chain integrity need definition, execution and investment now.

How can government, industry, civil society and academia cooperate to achieve Australia's international cyber and critical technology interests?

Policy makers should collaborate closely with multidisciplinary subject matter experts to investigate, prevent, and mitigate adverse uses of cyber technology. Simultaneously, policy makers should collaborate widely to expose and grow emergent opportunities.

In 2013, Australia ranked last in the OECD on the proportion of businesses which collaborate with research institutions on innovation.[14] Any approach which seeks to increase collaboration requires a long-term, patient approach to investment[15]. Case studies are provided below, with a note in several as to the timing of investment, which is on the order of decades.

Government needs to be clear in the objectives it sets, and the willingness it has to support them with longevity. DFAT should consider a few key principles or approaches to support much needed cooperation:

---

[10] https://www.first.org/about/mission, a global organisation supporting trusted computer incident response teams to better manage cyber security incidents and enhance incident prevention.
[11] https://www.quintessencelabs.com
[12] https://q-ctrl.com
[13] https://sqc.com.au
[14] Australian Department of Industry. Boosting the commercial returns on research: 2015
[15] D. Scott-Kemmis "*Myths, Crises and Complacency: Innovation Policy in the United States and Australia*" Dec 2018,

- **Adopt a mission-driven innovation approach,** for example as taken by the UK government and more recently by EU governments[16].
- **Narrative:** Develop a long term (20+ year), industrial cyberspace narrative, which has consistent national and international elements.
- **Support networked ecosystems:** Small-medium enterprises **(**SME's) and larger organisations as part of a decentralised, diverse and well-connected system, supported by
- **Education:** to enable growth of a highly skilled and higher-value labour market

DFAT's role here could be two-fold:

1. **Leadership:** providing insights from international better practice adoption to Australia to guide Australian businesses and agencies as they drive export opportunities.
2. **Coordination:** through close engagement with portfolio agencies (such as the Department of Home Affairs) and engagement with industry policy agencies (for example Department of Industry and Department of Defence), DFAT can provide a common understanding of the national drivers to cyberspace, and priorities for international competitiveness

DFAT could also partner wide and deep to co-develop the skills and capability Australia needs to build an advanced cyber assurance capability. In this way, it can support a trustworthy

[16] Mission Driven innovation: Mariana Mazzucato, *Mission-oriented innovation policy: Challenges and opportunities. Technical report*, Institute for Innovation and Public Purpose (University College London, 2017).

procurement strategy that may need to lean on core technologies and skills sourced outside Australia. As an example, the Center for Cyber Security and International Relations Studies (Florence, Italy) and the Embassy of the USA (Italy)[17] have been partnering to raise awareness on the risks and opportunities in cyberspace: providing virtual seminars on 5G, military escalation, cyber espionage & crime, misinformation and the implications for emerging technologies. These global partnerships are key to building a resilient Australian economy & society.

While cyber defence focussed, the learnings from the recent US Cyberspace Solarium Commission report[18] are interesting learnings for DFAT consideration, as an indicator of the importance other nations place on cyber security and the opportunity for leadership.

For DFAT and Australia to play a role and maintain engagement in cyber security, and demonstrate leadership especially for the APAC region, we need to have sufficient capability to add value. That's an opportunity for DFAT to engage in diplomacy on a grander scale: our neighbours may not have the capabilities to defend or prevent cyber security attacks, so an updated cyber engagement strategy must include this as an objective and measure of success.

We saw in COVID19 more prominently that international collaboration and shared understanding of norms in cyberspace are increasingly critical - DFAT's recent joint and public statement[19] is a step forward in that vein and these efforts need acceleration. But DFAT needs to do more: it is not sufficient to merely make a statement of values, without means to uphold them. Consequence management will be an important factor, made challenging with nation-state actors and attribution efforts. International efforts including the Open Ended Working Group (OEWG)[20] is a model to explore to help establish international protocols for peace-time and during conflict situations, what we expect to be protected from cyber operations (e.g. health sector, medical facilities, water facilities etc) and agreed terms for each context. Confidence-building and capacity-building in cyberspace should therefore be a key objective for DFAT's updated cyber engagement strategy.

DFAT's diplomacy role should include objectives to lead Australia and in a mentoring capacity to those in our APAC region (especially those that are unable to defend themselves in cyberspace due to resource limitations etc):

- Enhancing the deterrence to malicious cyberspace actors.
- Enhancing the resilience of the Australian economy & society to cyber-attacks.

[17] https://www.cssii.unifi.it/vp-89-il-center.html
[18] https://www.solarium.gov/report
[19] https://www.dfat.gov.au/news/news/unacceptable-malicious-cyber-activity
[20] https://ccdcoe.org/incyder-articles/a-surprising-turn-of-events-un-creates-two-working-groups-on-cyberspace /

- Enhancing the resilience of the Australian economy & society by supporting future industries, emerging technology research & development and skills in cyber security & related technology.
- Influencing government reform and adaptability in such a way as to increase its capacity & responsiveness to future-scape policy and strategy.
- Strengthening the cybersecurity capacity of private sector entities and raising the bar for public sector agencies especially critical infrastructure (health, voting systems, energy, financial etc).

A focus on speed, sustainability and industry engagement across emerging technologies is needed to shape our future society and economic prosperity. Cyber engagement to help focus on collaborations and partnership and frameworks to ensure Intellectual Property does not impede the ultimate objective - embracing entrepreneurs and fostering real commercial engagement. In the US, the military and public sector (see DARPA case study below), are strong investors and early customers for innovation and ground-breaking research & development. This has enabled deep-technology advancements to be achieved, which are not immediate but have created new industries (leading to multi-million/ billion-dollar businesses which employ higher grade skills and resources). Not only does this create a national advantage and support national security objectives, but it strengthens the supply chain, and the capital (finance and human capital) markets.

What policies and frameworks exist in other countries that demonstrate best practice approach to international cyber and technology policy issues?

The policies and frameworks of other countries are built in the context of national (self) interest.

> *The major economies are aligning policies in international agreements with perceived national interests: the United States is promoting an open architecture that aligns with the market dominance of its data-intensive firms, whose approach to systemic risks reflects private considerations only; the European Union is promoting sound regulation, which aligns with its primarily defensive interests; and China is taking advantage of the size of its internal market to develop a competitive digital economy.*[21]

For Australia, our approach is most likely a mix between these three extremes - we have few native industries, our 'local' market is predominantly China-based (which presents additional challenges given the cyber threat context and landscape) and our regulation approach is different to the EU. We must harness and empower our human capital with greater & higher-valued technical skills – skills such as IT infrastructure, computational literacy and cloud computing need to be combined with broader skills such as threat & risk analysis, critical thinking, project management, customer service and strategic planning.

[21] https://www.cigionline.org/articles/economics-data-implications-data-driven-economy

Developing coherent, business-driven long-term plans that leverage cyber-physical connectivity and data driven approaches is the key for Australia's success and its global leadership opportunity with cyber security engagement. The existence of clear, consistent plans which articulate digital objectives, without becoming lost in the 'how' or 'what', will support and ensure sustainable national industry investment and outcomes.

Key learning(s): a clear, articulate plan that describes agency gaps, and opportunities for industry investment, backed up with commensurate investment has helped drive significant growth in otherwise boutique Australian businesses

Opportunities to learn and adapt

Case Study: SBIR; a model for Australian Government Procurement

Considered the US Government's seed fund for innovation[22], the SBIR (small business innovation research) program and its parallel (STTR) technology transfer programmes were established and enacted into law in 1982. The funds (typically grants or contracts) are intended to assist small businesses advance research and development (R&D) where there is potential for commercialisation and can demonstrate alignment to specific U.S. government R&D requirements. These projects or ideas are typically those that may be considered too high risk for private investors, including venture capital.

The SBIR program agencies award monetary contracts and/or grants in phases I (up to USD$250K) and II (up to USD$750K, although an agency can award up to USD$1.7 million) of a three-phase program. The successful recipients own the intellectual property and all commercialisation rights. Companies such as Symantec, Qualcomm, and iRobot, Wombat Security Technologies (anti-phishing) have received funding from this program.

Key learnings: DFAT should consider increasing international collaboration with the SBIR programme coordinators to share success factors and programme design with Australian agencies and organisations - including but not limited to CSIRO, Industry Growth Centres, State Government Departments, Department of Defence and Department of Home Affairs.

Case study: Project Kessel Run, US Air Force.

Project Kessel Run, started in 2017 as a collaboration between the Defence Innovation Unit Experimental (DIUx – now DIU) and commercial partner company Pivotal, taking a technical concept to an operational product in 4 months in the US Air Force. Defence personnel paired with civilian developers to build iterative, software projects in an agile environment, for military outcomes. This has led to faster development and higher quality products. 'Jigsaw', a tanker planning software developed by Kessel Run, was created and operational in 120 days (which

[22] McFarland, Mondschein, Meers "Failure to launch: Australia, the United States and the threat of inefficient innovation" Nov 2017

would have taken 3,650 days under the Waterfall method of software development and acquisition) and cost the Air Force USD$1.5 million – a cost recovered in one week.

The software now saves the Air Force US$750K to US$1 million every week, and resulted in the cancellation of a Northrop contract for a 10-year project which was already 3 years behind schedule and had nearly doubled its budget to US$745 million.

Key learning: An extension of the Kessel Run project methodology may support DFAT's Cyber Engagement objectives - to build small and targeted partnerships with international organisations to achieve domestic objectives.

Case Study: DARPA (Defense Advanced Research Advanced Projects Agency)

Founded in 1958 in response to Sputnik, DARPA is a model for supporting cutting edge research & development with a 3-5 year plus lens. While focussed on Defence applications as the primary customer, DARPA has a long history of helping to create many multi-billion-dollar industries[23].

Its innovative investments have included the internet; RISC computing; global positioning satellites; stealth technology; unmanned aerial vehicles (“drones”) and micro-electro-mechanical systems (MEMS) used in everything from airbags, ink-jet printers to video games. CSIRO’s Data61 has been a collaborating partner for a number of DARPA sponsored projects.

The four key characteristics of the DARPA model are:

1. A series of relatively small offices, often staffed with leading scientists and engineers, given a considerable budget [US$3bn annual budget coordinated by 250 staff] and autonomy to support promising ideas. These offices are proactive rather than reactive and work to set an agenda for researchers in the field. Their goal is to create a scientific community with a presence in universities, the public sector and corporations that focuses on specific technological Challenges.
2. Funding is provided to a mix of university-based researchers, start-up firms, established firms and industry consortia. There is no dividing line between ’basic’ and ’applied’ research. DARPA personnel are encouraged to cease funding where there is little progress and reallocate resources to other groups that have more promise.
3. The agency's mandate extends to helping firms get products to the stage of commercial viability. DARPA provides organisations with assistance that goes beyond research funding.
4. DARPA’s objectives also include using its oversight role to correlate ideas, resources and people across the different parts of the research and development ecosystem
5. It sets ambitious goals - harnessing cutting-edge science, engineering to solve complex problems or forecast/ create new opportunities. This creates focus and inspires significant creativity in the teams
6. Independence - the autonomy to select and execute projects, enables fast-decision making in what is typically, high-risk ideas.

[23] Biercuk, “Next steps for Australia’s Defence Innovation: Lessons from DARPA” Oct 2017

As an example, DARPA recently established a new programme to combat attacks that are designed to interfere with the automated systems - Guaranteeing Artificial Intelligence (AI) Robustness against Deception (GARD). A multimillion-dollar, four-year initiative with the objective to create defences for sensor-based artificial intelligence — e.g. facial recognition programs, voice recognition tools, self-driving cars, weapon-detection software and more.

Key learning(s): This is the sort of moon-shot thinking & investment that is required - but Australia cannot do so alone, so cyber engagement & collaboration at an international scale is critical as is correlating and mustering local ecosystems to 'play'. This can assist in capacity building domestically for skills & experiences we sorely lack or are unable to organically build ourselves.

Case Study: Finland

Supported by continued investment in education, research and innovation, Finland achieved a widely acclaimed transition from a largely resource-based to a leading knowledge-based economy shifting towards high-technology manufacturing and knowledge-based services, over a period of nearly 15 years.

Finland was hit hard by the global economic crisis in 2009, and disruptive technological change contributed to the decline of Nokia's handset business and a sharp drop in exports of IT goods. Subsequently, Finland lost comparable positioning in terms of productivity and competitiveness. Industrial restructuring led to a steep decline in business R&D expenditure. The new vision for Science Technology and Innovation (STI) driven by economic needs and societal challenges (including energy efficiency, population ageing and climate change) saw their Research Innovation Council (RIC) playing an important role.

Key learning(s): Finland is seeing its government-led R&D investment programs showing signs of sustainability, so DFAT may find their tiered approach to public-private investment a model for further analysis and possibly adapting these to the local context.

Case Study: Ireland

Ireland has a highly mobile SME community, with a high intensity of IT investment, taken as a per-capita business investment. During the current COVID-19 crisis, the Irish Scientific Investment agency Science Foundation Ireland (SFI) used its investment framework to develop 'fast turnaround' industry linkage programs based on:

- Open on-going proposal deadlines: meaning that industry is not captive to annual research funding cycles.
- Fast turnaround: proposals are reviewed by international reviewers within 10 days of submission.
- Medium investment: proposals do not require matched industry support and are focussed on up to 1 million euro.

- Fast results: proposals are required to demonstrate initial proof-of-outcomes within 30 days.

Key learnings: The above linkage programmes could significantly uplift existing local research & development protocols and plans. Additionally, the SFI proposals are funded to address immediate national requirements, with a view to driving commercialisation and export industry in the medium (2-3 year) term - which could encourage greater and purpose-led industry collaboration.

What technological developments and applications present the greatest risk and/or opportunities for Australia and the Indo-Pacific? How do we balance these risks and opportunities?

Access to digital technology is unequal across even suburban Canberra[24], let alone between developed Australian capital cities and poorer nations to our north and east. The impact of technological advances on cyberspace 'haves' vs the 'have nots' is likely to be profound.

Startups and emerging technology-led businesses are one of the means to develop the critical skills, technology and economic opportunities for our future generations. They are often overlooked in Australia due to the overwhelming culture & appetite for 'not built here.' A similar 'not already used here' problem also exists in public procurement -- where a 'new' vendor may find themselves asked to provide references and evidence of a new product already being used by some other Australian Government agency. This procurement barrier can be overcome by large corporations - who can provide 'free' proof of concepts to agencies to establish themselves. This is not a feasible approach for newer and smaller businesses.

The authors have current and real experiences of doing just that and supporting the local ecosystem.

Australia can and should play a significant role in the research, development and commercialisation of key cyber security technologies and capabilities. Australia is a creative nation, but many reports point to our failure to commercialise this technology. DFAT has the opportunity to partner and broker with other agencies (domestic and international) including Austrade, to effect economic opportunities in key cyber and cyber related technologies. In reality, Australia cannot manufacture or operationalise all its critical cyber security needs, so it must build sufficient capacity and capability to be a sophisticated buyer.

Examples of technological developments for Australian investment and R&D support should include consideration of AI, quantum computing, privacy & cyber international law, privacy enhancing/ enabling technology, 5G/6G (and next generations), cryptography, and data integrity technologies (think the wave of misinformation and disinformation that we've seen lately with

[24] Driving for more than an hour in almost any direction from any suburb in Canberra will result in loss of 4G and 3G data signal as one Author can attest.

political elections, COVID19 and more to drive social and economic unrest). Digital and computational literacy will be important drivers of equality.

The technological advances in Quantum Computing - including Google's open source Quantum Deep Learning toolkit[25] are already driving increases in capacity to store and process data. Although quantum computation is not yet mainstream, it is already possible to simulate significant Quantum computers, albeit at moderate expense. Combining nearly limitless processing capacity, nearly zero-cost storage and ubiquitous network access means that computing may be able to solve most 'difficult' problems.

The opportunity: our capacity to use evidence to achieve optimal policy objectives, based on real data may take less effort than the current 'experience based' approaches.

The risk: the analysis of private data, the risk of 'poorly designed' or 'unethical' AI's and the malicious application of AI (for example deep fakes[26]) and attacks on AI[27] by cyber threat actors (using the tools for malicious intent). The old saying 'no-one knows you're a dog on the Internet' has greater potential in an algorithmic world.

This is worse for the cyberspace 'have nots' who are unlikely to have the skills to assure AI developments, deployments or results. Examples of poorly designed (biased) AI or maliciously targeted AI[28] through to the active malicious use of AI[29] are currently few, albeit concerning. Startups are emerging to develop commercial 'fakes' which present the likeness of celebrities to endorse advertised material. The existence of such false digital twins presents a demolition of trust. At a time where traditional trust frameworks are disintegrating globally, there is significant opportunity both economically and for social good, to build:

- capability to identify and verify trusted information and components; and
- higher assurance and trustworthiness in our partnerships, supply chain, platforms and components and information.

The have's vs the have-nots: mis-managed development of cyber dominant economies is likely to centralise wealth to fewer nations or, perhaps, fewer organisations and individuals. The rise of 'superstar' or monopolistic firms with platform-based solutions, such as Google and Facebook drive a net reduction in the economic share of the average worker, even though those organisations may pay higher than average wages.

> *The declining labour share has been coupled with a slowdown of economic growth, which means declining pay and job opportunities for the average worker. In effect, workers are getting a shrinking slice of a barely expanding pie.* [Reenan, Patterson 2017[30]]

[25] https://ai.googleblog.com/2020/03/announcing-tensorflow-quantum-open.html
[26] www.csoonline.com/article/3293002/deepfake-videos-how-and-why-they-work.html
[27] https://spectrum.ieee.org/automaton/artificial-intelligence/embedded-ai/adversarial-attacks-and-ai-systems
[28] https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html
[29] https://arxiv.org/pdf/1802.07228
[30] https://hbr.org/2017/05/research-the-rise-of-superstar-firms-has-been-better-for-investors-than-for-employees

The worker in remote Australia or Western Papua may not see the economic benefit of an increasingly digital economy: they may be left with the crumbs of a much richer society which can afford to be better educated (on the risks and trade-offs), have greater and more diverse opportunities and which will fail to notice them as they have a negligible digital footprint.

Digital inequalities pose similar risks to Australia and our neighbours as does economic, education or infrastructure inequality.

A number of countries have publicly stated their increased investment in offensive cyber strategies and capabilities. The current environment has shown that the attribution of state v non-state threat actors is becoming difficult, as the weaponization of data[31] continues. Cyber diplomacy is a key component to helping organisations and public sector agencies navigate this situation and manage their defensive posture - Australia's signed agreement with China in 2017, with commitment to 11 international norms in cyberspace is a great first step. While necessary, diplomacy is not sufficient. How will this be monitored and how will suspected or known breaches be managed?

Australia has the opportunity to play a leadership role to strengthen APAC nations' resilience to cyber-attacks, while at the same time enabling our economy to do the same (we must realise that Australia while an island, is not so in a digital sense - we are connected in a network of systems and interdependencies, so leadership and collaboration in the region is critical notwithstanding the cyber threat environment and increasing geopolitical complexities/ sensitivities). And Australia is not immune to the risk of being left behind by more dynamic and digitally innovative economies elsewhere in the region and world.

Australia's opportunities are vast and valuable. DFAT's updated cyber engagement strategy and execution is in the driver's seat to accelerate those opportunities through partnerships, collaborations and leadership on the global stage.

--end--

[31] For example, www.wired.com/story/eternalblue-leaked-nsa-spy-tool-hacked-world