Australian National University

National Security College
POLICY **OPTIONS** PAPER
NO 21, SEPT 2021

Data-Driven Technology and National Security: Enhancing Government Collaboration with the Private Sector

by Alasdair Gordon, CEO of Ecosse Global

Key points

- To harness rapid advances in machine learning, data analytics, automation and related data-driven technologies, Australia's intelligence and security community must broaden and deepen partnership with the private sector.
- Small and medium enterprises (SMEs) are critical sources of innovation but face unique challenges to engaging with government – especially intelligence and security agencies.
- The key obstacle to national security innovation is culture, not procurement policy.
- Given fast global R&D cycles and Australia's dynamic national security environment, if private actors wait for government to specify requirements, they will be left behind.

Recommendations

- The Office of National Intelligence (ONI) and other relevant agencies should continue to promote communication across government to build a common picture of technology needs and solutions.
- Agencies should enhance two-way information-sharing between industry and government, including via an annual Industry Roadshow and targeted industry briefings on emerging priorities, and through a more formal program of education for the business sector of the challenges in working with the intelligence and security community.
- Agencies should seek guidance from the Department of Finance on how existing procurement rules can support flexible and streamlined government/industry engagement on data-driven technology solutions.
- Industry should create an online marketplace for the intelligence and security community where industry can proactively showcase capability.

To remain fit-for-purpose in the twenty-first century, intelligence and security agencies, which includes Federal and State law enforcement agencies, must be fast adopters, and effective users, of data-driven technologies. But governments can't go it alone. Government is not the main creator or customer of twenty-first century innovation. The twentieth century 'military-industrial complex' model of innovation – based on core relationships with several large primes – will not meet key requirements in a data driven age.

Today, data-driven innovation is just as, if not more, likely to come from a gaming start-up or a mid-sized data analytics firm, as it is from a mature multinational with decades of intelligence/security sector experience. This makes SMEs – already an engine of Australia's prosperity – also vital to our security.

A core challenge for intelligence and security agencies, will be building engagement and genuine partnership with the private sector. This exchange must be win-win; industry can't be compelled to the table and needs to see real value in engaging with the intelligence/security sector.

Data-driven technology is different

Data-driven technologies, such as artificial intelligence (AI), machine learning, data analytics, cloud computing and automation are critical to twenty-first century security. But the nature of these technologies, and the innovation system in which they are developed, is markedly different to the twentieth century government policy, processes and culture for technology procurement and deployment.

A new innovation ecosystem

Today's innovation ecosystem is fundamentally 'open'; innovation can come from anywhere and spreads quickly, and widely.[1] Big, medium and small players across all sectors have significant roles to play. Data-driven technologies are also largely multi-use, yielding applications across the industrial, consumer, social, defence and other sectors. Governments are not the biggest or wealthiest customer. Further, global R&D cycles are accelerating, compressing the time governments have to identify and understand technological developments.[2] This necessitates new, more flexible approaches for integrating technology across government.

The power of small

SMEs are increasingly critical players in twenty-first century innovation. Because of the multi-use nature of tech, many of our most innovative businesses don't see themselves as operating in the security space. They may not have engaged with intelligence and security agencies – or even government – before. And they are unlikely to have large teams devoted to business development, legal compliance, or contracting.

Speed, scale, and sustainability

Data-driven solutions tend to work best at scale; one reason, for example, why many governments now have 'cloud-first' policies. But twentieth century structures – from departmental silos to agency-level procurement processes – can impede cloud-based, scaled solutions. Previously, agencies have sought bespoke solutions to address short-term needs. But today, an enterprise strategy can deliver longer-term solutions at scale, which target priority problems.

Finally, data-driven solutions are software-reliant, the problems they address are complex, and national security agencies' needs and operating environment are increasingly dynamic. This is driving an evolution in the relationship between agencies and industry – from a model of one-off purchases to longer-term partnerships of adaptation and continuous software refinement.

Culture and organisational lag

Australia's intelligence and security community is not yet 'one enterprise' that can engage seamlessly with the technology marketplace. Australia is not alone. An expert working group convened by CSIS recently concluded that the US intelligence community entered 2021 "flatly behind the technology curve" with its adoption and integration of AI and associated technologies remaining "piecemeal and episodic".[3]

In Australia there are few formal mechanisms for:

- agencies to share information in a timely way to shape industry understandings of government needs, priorities, and context; and
- industry to proactively inform and shape government requirements, including by showcasing their suite of capabilities.

Rigid processes

In the fast-paced world of data-driven technology, businesses will be most successful if they anticipate customer requirements and build capability in advance to meet those requirements. However, the government's 'approach to market' process is a rigid vehicle for identifying relevant innovation, and innovators.

Every response to an approach to market represents a significant cost, both in direct terms, and in opportunity cost. Businesses that can offer government something useful, but that may not meet all the specified requirements, may choose not to participate, potentially depriving government of important capability.

For businesses looking to start engagement with government, procurement panel processes can be a highly resource-intensive often multi-year process. Even within departments, there are often multiple panels (with differing requirements) that a new entrant might need to engage with. There is a need to continue to standardise and simplify procurement processes across agencies, and to broaden the talent on panels.

Silos

Many of the intelligence and security community's technology investments are made "by individual agencies with individual suppliers".[4] Funding cycles create perverse incentives for agencies to create barriers to collaboration, while there is a commercial incentive for industry players to contract with agencies separately.

Risk-aversion

A culture of risk-aversion is a barrier to a more experimental and flexible approach to technology use by intelligence and security services. There is a perception that senior leaders do not sufficiently incentivise the types of calculated risks – and toleration of failure – needed to adopt effective data-driven solutions.[5] Similarly, multi-year innovation projects often need 'champions' inside government to give them high-level support. Worthwhile projects have faltered when champions can't be found or move on to new roles.

Scattergun industry engagement

Procurement silos and lack of consistent information-sharing means that industry approaches to government can be ad hoc and inefficient. These challenges place a unique burden on SMEs, due to their small size and thinner networks into government. Further, SMEs are reluctant to expose their ideas to government outside of formal procurement processes, due to concerns that their intellectual property might not be protected. There are further barriers to proactive industry engagement, especially from SMEs. Some perceive that the security space is too niche, while others are held back by misperceptions about security requirements and risks (and who bears them).

A better way: 360° information-sharing

Across government

The government has made important steps towards presenting an enterprise-level front to industry. The National Security Science and Technology Centre (NSSTC), housed in the Defence Science and Technology Group (DSTG), is charged with raising awareness across agencies of their respective investments, to enable a more collective and efficient approach to achieving their capability goals.[6]

The NSSTC is an important first step, but there is a need to go further. This doesn't require an overhaul of federal procurement law and policy; it's about communication and culture. Importantly, information-sharing should extend beyond intelligence and security agencies. Other central and service-oriented departments, as well as state and territory governments, will share similar problems – and be building their own capabilities to address them – and need to be included in the drive towards cooperation.

To industry

The government has articulated National Security Science and Technology Priorities[7] to drive alignment and collaboration across Australia's innovation ecosystem. This can now be taken further. There is a clear need to provide mechanisms outside of the formal procurement process to enable industry to better understand government, and the benefits of doing business with it.

In particular, the NSSTC, supported by a range of departments and agencies, should conduct an annual Intelligence and Security Industry Roadshow in state capitals. This would build awareness about the priorities, the background that led to them, and Australia's broader national security context and procurement processes. A roadshow should also include information about the budget available to support innovation against the priorities, to make opportunities more tangible and relevant to SMEs. Agencies should also expand efforts to offer targeted briefings to high-priority innovators on emerging priorities and requirements.

At the same time, a more formal industry funded program to enhance industry understanding of the intelligence and security community, including the challenges in doing business with intelligence and security agencies, should be implemented.

To government

Government should consider creating an online Intelligence and Security Marketplace to allow industry to proactively showcase capability to agencies. This would have the benefit of streamlining access to government and would not favour vendors with more established government networks. It could also reduce the costs to SMEs of government engagement.

Building genuine partnerships

The National Intelligence Community (NIC) Science and Technology Advisory Board, created in 2017, is helping to drive a more coordinated approach to capability development across the NIC. The Board helps the NIC to anticipate and develop future enterprise-wide needs, including via a new Joint Capability Fund and Intelligence Capability Investment Plan.[8] The Department of Defence is simplifying pathways to industry partnership and co-development in areas including algorithms, data analytics and autonomy.

Accelerating industry/government collaboration on data-driven technology is a global trend. Five Eyes partners are actively "building bridges" between private sector innovators and defence/security agencies.[9] Authoritarian competitors are increasingly integrating their government and innovation sectors: for example, China's "military-civil fusion" strategy lets China rapidly apply emerging technologies to security purposes.[10] Australia's challenge is to build a more effective system of public/private innovation that enables national security agencies to harness the creative dynamism of the free market.

Agencies can explore vehicles for industry engagement and procurement that help to manage government perceptions of risk and reduce industry's costs and perceived risks of engagement on industry, especially SMEs. These include:

- ***Sandbox experiments:*** Before a formal procurement process is commenced, 'sandbox' experiments offer flexible vehicles to test industry solutions. These can be run on segregated or simulated datasets, minimising risk.
- ***Accelerator programs:*** Government and industry can share R&D risk and costs. For example, government can use accelerator programs as a vehicle for matching good ideas, which may not yet be mature enough for significant government investment, with venture capital.
- ***Co-developments:*** In the multi-use technology age, industry and government often share problems and missions without realising it. Co-development spaces, such as US Cyber Command's DreamPort, and the Data to Decisions Cooperative Research Centre model in Australia, can offer genuine win/win outcomes for industry and government, and a mechanism of managing risk and security.

- ***Streamlined processes for SMEs:*** Agencies should consider offering simplified, low-cost procurement options for smaller and less experienced players. For example, the US Defence Innovation Unit offers a streamlined format for responding to Defence solicitations, whereby industry can express interest via a 5-page brief, or short slide deck, before being invited to make a more formal pitch.[11]

Maintaining Integrity and Probity

Most of the above options do not require legislative, or even significant policy, change. Australia can get more value from its current procurement framework. Agencies should seek guidance from the Department of Finance on how existing procurement rules can be used to maximise benefit in the data-driven age.

There is particular need for clarification on the rules for 'pre-procurement' engagement. One concern is that participation in these activities can disadvantage industry; for example, that those involved in informing and shaping requirements may be later excluded from a tendering or procurement process for probity reasons. Agencies should proactively seek advice – and share best practices among each other – about how to safely work within procurement rules to drive flexibility, while maintaining ethics and core values.

Notes

1. Audrey Kurth-Cronin, *Power to the People*.
2. DST, National Security Science and Technology Priorities 2020
3. Maintaining the intelligence edge, CSIS, https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/210113_Intelligence_Edge.pdf
4. National Security Science and Technology Policy and Priorities, https://www.dst.defence.gov.au/sites/default/files/publications/documents/NS-S%26T-policy-and-priorities.PDF.
5. A similar assessment has been made in the context of the US intelligence community: https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/210113_Intelligence_Edge.pdf
6. National Security Science and Technology Centre, https://www.dst.defence.gov.au/nsstc
7. DST Group, National Security Science and Technology Priorities 2020
8. Office of National Intelligence, Enterprise Management, https://www.oni.gov.au/enterprise-management
9. CSIS Technology and Intelligence Task Force, https://www.csis.org/programs/international-security-program/csis-technology-and-intelligence-task-force
10. CSIS Taskforce on Intelligence Innovation
11. Procurement Technical Assistance Center, Defense Innovation Unit: Merging Innovation with Acquisition, https://www.norcalptac.org/about-us/news/defense-innovation-unit-merging-innovation-acquisition

About the editor

This paper has been edited by Katherine Mansted, Senior Fellow in the Practice of National Security at the ANU National Security College. The paper is based on a series of workshops conducted in 2020 with industry leaders and policy practitioners, which was supported by Ecosse Global. The NSC is independent in its activities, research and editorial judgment and does not take institutional positions on policy issues. Accordingly, the views expressed in this publication should not be taken as reflecting the views of any government or organisation.

About this publication

Policy Options Papers offer short, evidence-based and forward-looking insights and recommendations for policymakers on topical national security issues facing Australia. Every paper in the series is informed by consultation, and reviewed by practitioners and academic experts.

About the National Security College

The National Security College is a joint initiative of The Australian National University and Commonwealth Government. The NSC offers specialist graduate studies, professional and executive education, futures analysis, and a national platform for trusted and independent policy dialogue and contestability.

T +61 2 6125 1219

E national.security.college@anu.edu.au

W nsc.anu.edu.au

@NSC_ANU

National Security College

CRICOS Provider #00120C