National Security Science and Technology Workshop – 5 May 2014 Summary of key outcomes

This workshop was the second in a series of workshops aimed at engaging and consulting with the national security science and technology (S&T) community on the development of a national security S&T policy and program. The policy and program aim to achieve a coordinated whole of government approach to prioritising, planning and funding national security S&T.

The morning session presentations provided context to syndicate discussions on Policy and Governance, and proposed national security S&T priorities – Border Security and Identity Management; Preparedness, Protection and Incident Response; Investigative Support and Forensics and Intelligence Exploitation. A separate workshop was held on 6 May to discuss the national security S&T priority - Cyber Security.

Syndicate: Policy and Governance

Policy objectives

- Overall the proposed policy objectives[1] were accepted as being appropriate.
- Other suggested policy objectives:

[1] Define Australia's NS S&T priorities for next decade; Coordinate efforts to best take advantage of investment in S&T and address critical gaps to address immediate and future national security capability, operational and policy needs; develop and support S&T collaborations and networks that bring together, under a shared vision, the best in industry, academia, PFRAs and government; and create a public and private investment partnerships in national security S&T through a Program that accords with Government priorities and capitalizes on our broader innovation system and international linkages.

    - Accelerating innovation to address national security needs and to build national capacity (ie. facilitating commercialisation and generating spin off companies or growing current companies),
    - Leveraging from international partnerships (ie. identifying Australia's unique capabilities and expertise and what capabilities can be met by other countries).
- Defining the scope of national security was seen as an imperative to identifying national security S&T needs (including emerging needs). This guidance should come from the government's national security policy.
- We must clearly articulate how we will achieve our policy objectives including how we will:
    - address national security S&T priorities in a coordinated way, while taking advantage of Australia's S&T capabilities and addressing our S&T capability gaps;
    - fund the work to address national security S&T priorities.
- Rapid acquisition – policy must put in place mechanisms that deliver solutions in a timely (short term) manner.

Prioritisation

- There was general support for the proposed national security S&T priorities meeting national security S&T needs.
- In setting priorities, it was seen as essential that we look at national capability and capacity, what resources/capabilities we might need to build within Australia and what might be available through international partnerships.
- "Transfer enablers"; transverse capabilities" will be important to avoiding stovepipes.
- Changing priorities to factor broader perspective may allow leverage of external resources to deliver S&T to meet national objectives.
- Priorities need to address needs of the range of national security stakeholders, not just Government.

Governance

- The governance structure must suit the program being developed and delivered.
- The proposed Steering Committee should include a representative from Department of Finance (linkage between government and funding), and broad representation from industry and academia. Many Government stakeholders are not included on the current list – e.g. Health, Agriculture and states and territories (e.g. first responders and other state based elements of National security system).
- Private sector is not just an S&T provider but is a stakeholder who manages critical infrastructure and therefore should be represented at the senior level in that capacity too.
- There is a risk the Steering Committee could become unwieldy and dysfunctional if it is too big and tries to represent all stakeholder groups, who will all have different agendas and priorities and may never agree.
- In terms of managing conflict of interest within the Steering Committee, there are many extant models (Australia and overseas) that successfully manage this – e.g. DMO (Conflict of Interest register, Non-Disclosure Agreement, exclusion from certain discussions etc). A successful (and potentially transferable model) is the Australian-New Zealand Counter Terrorism Committee.

- Another governance option discussed was a Board, rather than a Steering Committee. A Board could be smaller and independent, possibly operating with an Advisory Committee/Council that brings in expertise where needed. The Board could have members with commercial/business, policy and technology expertise, and need not all come from the national security community.

Role of DSTO

- DSTO has many roles - S&T Provider; coordinator; bilateral/multilateral arrangements; leverage other international arrangements (e.g. TTCP).
- DSTO should bid separately for project funds as other S&T providers will. DSTO should not be gatekeeper, but advise, direct, mentor, coordinate, facilitate.
- Australian Signals Directorate (ASD) has whole of government security role. There may be lessons learned from ASD's experience/situation that could be applicable for DSTO.

Industry and academia engagement

- Interaction previously has been poor.
- To improve industry and academia engagement we need to understand what will drive them to engage and collaborate (e.g. academics – promotion is dependent on securing prestigious research grants and publishing in quality journals)
- Need to recognise that "industry" plays many roles – S&T provider, operator of national infrastructure, funder etc.
- Industry must be brought in earlier in the S&T process. Need to investigate the utility of other models such as the Rapid Prototype and Development and Evaluation program (RPDE) that bring industry into Defence capability development at an earlier stage.
- Other engagement models to investigate:
    - Deputy Vice Chancellor Research model
    - CRC model
    - Hague Security Delta

Barriers to engagement

- Attracting industry R&D investment. Parent companies have huge R&D budget but the business case for investment in Australia is difficult. Advantage in getting industry involved earlier in formulating program so they can build case for co-investment.
- Probity. Manageable by putting probity arrangements in place if necessary to keep industry at arms-length from procurement decisions etc.
- Timeframes. Lengthy periods between between industry submission and contract awarded. Academia may take five years to complete study. ARC funding cycle can preclude long term perspective and ability to mature technology from low TRL levels.
- Barriers to universities accessing industry funding.
- Better approach is to tender work so it encourages industry linkages.

Co-investment

- A 50:50 split is not recommended (could take focus away from the real issues). Perhaps user agencies (ie. government) should contribute more (very challenging in the current budget situation).
- There will be an expectation that if collaborators contribute, they should get something in return.
- Other models:
    - RPDE type models (fixed fee plus performance benefit)
    - US 'hub and spoke' model – bilaterals with 5 nations (AUS, Singapore, Israel, UK, Canada).
    - CRC's. Driven by end-user and more attractive to industry investment.
- Absence of a funding mechanism between ARC grants and CRC's.
- There is funding available from Venture Capital. Universities don't really chase after this source of funding. Links back to university's method of advancement for academics and low risk appetite.

Measures of success

- How many ideas funded and made it into service.
- Marketing successes – awareness and learning from failures
- Outputs, usage, impacts, export successes
- Universities measure of success will include level of engagement (ie. being at the table), success in transferring knowledge and number of PhDs produced.
- Giving industry opportunities
- Success of funding will be development and maintenance of collaborative partnerships.

Syndicates - S&T Priorities

Border Security and Identity Management

DSTO POC: Dr Duncan Craig

The Motivating Challenge:

Preserving Australia's border integrity key challenge for Government. The projected growth in people and cargo movement across Australian borders is challenging Customs' ability to identify and assess risks and to conduct timely interventions.

Scope

- Broad, covers lots of different things.
- 'Border continuum' – physical borders, maritime borders, international borders.
- Need to manage different risks along this continuum (e.g. parcel surveillance at borders)
- Tension between facilitation and security.
- Identity management overlaps with other themes – 'Investigative support and forensics', 'Intelligence Exploitation.'

Challenges

- With cargo and people traffic increasing, the challenge is to automate the collection, management and analysis of an increasing volume of data.
- There are challenges relating to technologies to detecting and tracking illicit goods (e.g. people and cargo).

Priorities

- Better data acquisition, processing, analysis and detection.
- Data integrity.
- Awareness of reputation and legislative context.

Industry and academia engagement

- Difficulty in attaining security clearances to support collaboration (especially time delay).
- Level of investment in Australia versus US (industry investment in R&D in US for higher TRL work).
- Need longer term commitment from government and not just focused on short term objectives
- Future support to the National Border Targeting Centre.

Intelligence Exploitation

DSTO POC: Dr Dale Lambert

The Motivating Challenge:

The deluge of available data from heterogeneous sources is challenging the capabilities of agencies to extract actionable intelligence, requiring the support of automated data analysis and representation tools.

Scope

- It was suggested that the Sub-Program scope should focus on agency engagement, stakeholder requirement matching and tailored technical solutions with a roadmap for implementation. Broadly, this may involve innovative data management of collected information through to analytical methods to achieve actionable intelligence.
- It was observed that stakeholder agency interests cover S&T support for their 'tradecraft' as well as information sharing within secure frameworks.
- In identifying the technical solutions, it was considered important to consider national and international best-practice within and *beyond* the sector (i.e. outside Defence and intelligence communities) e.g. commercial operations (e.g. supermarkets).
- It was noted that some additional activities may include defining the capability framework, further gap analyses and further Sub-Program roadmap development.

Coordination, delivery and governance

- It was noted that given the plethora of available diverse coordination, delivery and governance models it is important to identify an appropriate model for this activity.
- It was agreed that a high-level steering committee comprised of relevant agencies should have oversight of the activity.
- It was agreed that the roadmap for S&T provision needs to be scrutinised by a body of stakeholders with specialist oversight to ensure value for effort.
- It was noted that there is potential for the D2D Collaborative Research Centre (CRC) to participate in requirements gathering.
- There was some suggestion that some of the problems in this area are less 'greenfield' and more 'brownfield' in nature. This is in the sense that there is an existing body of work and expertise in this domain within stakeholder agencies, some CRCs and academia.
- It was also noted that it may be expedient to leverage other established programs where synergies exist. It was asserted that a challenge will be to incentivize academics to participate.
- It was suggested that it may be worth reviewing alternative models such as to incentivize engagement and collaboration.
- The importance of maintaining an open approach to alternative governance models was also recognised as potentially beneficial.

Industry and academia engagement

- Facilitating public–private investment, industry engagement and commercialization opportunities were seen as potentially valuable.
- Consideration was given to the potential of the Australian Space Policy Unit is another model of collaboration.
- It was noted that the Australian Research Council represents another model for engagement with academia but that this has very long application times (12-15 months) and relatively low success rate.
- It was also noted that CRCs are an appropriate mechanism for engagement with industry, but that the application process is relatively slow.

Investigative Support and Forensics

DSTO POC: Dr Andrew McAnoy

The Motivating Challenge:

Novel, adapted and complex methods used by terrorists and perpetrators of nationally significant crimes creates an ongoing need for S&T assisted solutions to detection, investigation and prosecution.

Scope

- "S&T supporting investigation of nationally significant and transnational crime and domestic terrorism" 'Transnational' and 'domestic' are not needed in scope statement.
- "Serious and organised crime" was discussed as a descriptor but "nationally significant" seemed to provide an appropriate distinction for what should be consider under NS S&T program.
- "Attribution" was considered a key descriptor to be included scope.
- Scope of program should not be too restrictive
- Investigative Support and Forensics (ISF) issues are "broader than just S&T" and overlaps with other sub-programs.
- S&T Program should be
    - operationally focussed
    - reactive as needed
    - proactive where possible.

S&T requirements

- For many participants, this was their first involvement in the process and it was agreed that this syndicate discussion would not give enough time to sort through S&T requirements even at a high level.
- Process needs to include
    - What we need
    - What we deliver
    - Assessment of priority

- Discussions around ‘project’ and ‘capability’ outcomes, delivery of ‘product/widget’ vs building ‘knowledge/capacity’.
- The process needs to be flexible allowing for short term projects delivering tangibles and mid-long term projects/ themed programs that build/maintain national capabilities or networks (still with NS benefit).
- Short term (low $$ or low risk) need quick approvals and outcomes (e.g. assessment and early adoption of technology/device).
- “Creation”, “Adaption” and “Adoption” useful descriptors for work under Investigative Support and Forensics (ISF).

Coordination, delivery and governance

- Funding (both $$ and in-kind) was clearly an issue.
- States and Territories need to be represented – not only at working level but at higher oversight levels – to get required buy-in from their respective agencies (e.g. state police).
    - Australia-New Zealand Policing Advisory Agency (ANZPAA) is an important stakeholder.

Industry and academia engagement

- Clear guidance to S&T providers is required, and they need to be part of the process to determine/refine what is possible and can be delivered.
- Benefit in user agencies to collectively prioritise S&T requirements for S&T providers, with greater clarity for both short and long term needs.
    - Would also allow for more appropriate choice of S&T providers for specific projects.

Other issues

<u>Future Requirements + Workshop</u>

- Further workshops will be held at later stage to elicit user requirements and further develop/refine ISF sub-program.
    - May be conducted as part of other activities being conducted later in the year.
- Some user agencies indicated they already had done some work that will help inform the ISF requirements.
- ISF overlaps with most other sub-programs to some extent with most obvious being Preparedness, Protection and Incident Response (PPIR). Explosives and CBRN are main threats under ISF (now listed as “ISF Centrepieces”) so need to be clear how working groups (WGs) operating under PPIR would work. Two considerations -
    - Separate Explosives and CBRN WGs under ISF
    - Explosives and CBRN WGs report to both SPOCs
    - Combine ISF and PPIR.

Preparedness, Protection and Incident Response

DSTO POC: Dr Norbert Burman

The Motivating Challenge:

Ensuring Australian agencies are appropriately equipped and prepared to effectively and safely respond to events of national security significance, such as a terrorist attack on critical infrastructure or mass gatherings.

Scope

- Greater focus of the scope, including name change. Re-scope to include:
  - Natural hazards
  - Home Made Explosives (HME)
  - CBRN

Program delivery

- Three-tiered phased program that demonstrates what the benefits are. Identify exemplar projects for:
  - Short – quick wins with High Priority identified (ready to go) projects (e.g. biohazards, HME)
  - Medium –identification of end user S&T priority needs (using extant coordination mechanisms such as ANZCTC, ANZEMC, TISN)
  - Long – capability/ capacity audit to ensure that there is clear understanding of what exists or is in development
- All of the projects are informed by: end users (e.g. Agriculture, Health, Industry, Defence); national security risk assessment; national security capability stocktake; where S&T addresses a capability need.
- International cooperation can assist in achieving the aims of the program.

Other issues

- Triple bottom line benefit analysis – people, economy, and environment.
- Redeploying capital and in kind contributions we already have access to.
- Participants must be willing to collaborate across agencies.
- Connect to a greater range of potential users (utilising appropriate fora, eg ANZCTC, ANZEMC and TISN) and gain their input as to the top S&T capability requirements (Note that a key assumption here is that we will rely on existing fora to gain inputs from the States and Territories).
- Develop a greater understanding of risks regardless of hazards.
- Determine whether the risk assessment element should remain within PPIR.
- Determine capability gaps and what S&T can do to assist.

Organisations represented

Aerospace Concepts Pty Ltd

ANZ Bank

Attorney General's Department (AGD)

Australian Centre for Cyber Security (UNSW Canberra)

Australian Crime Commission (ACC)

Australian Customs and Border Protection Service (ACBPS)

Australian Federal Police (AFP)

Australian Institute of Marine Science (AIMS)

Australian National University (ANU)

Australian Nuclear Science and Technology Organisation (ANSTO)

Australian Research Council (ARC)

Australian Transaction Reports and Analysis Centre (AUSTRAC)

Bureau of Meteorology (BOM)

CISCO

Commonwealth Scientific and Industrial Research Organisation (CSIRO)

Cooperative Research Centres Association

D2DCRC/Defence Systems Innovation Centre

d3Medicine

Deakin University

Department of Defence

Defence Materials Technology Centre (DMTC)

Defence SA

Defence Teaming Centre

Department of Finance

Department of Foreign Affairs and Trade

Department of Health

Department of Industry

Department of Infrastructure and Regional Development

Dunns4 Consulting Pty Ltd

Edith Cowan University

Flinders University

Geoscience Australia

KPMG

Lockheed Martin

National Health and Medical Research Council (NHMRC)

National Institute for Forensic Science

NBNCo

NEC

NSW Police

Queensland University of Technology

Rapid Prototyping, Development and Evaluation (RPDE) Program

SAGEM Australia

Thales

Universities Australia

University of Adelaide

University of Melbourne

University of Tasmania

US Combating Terrorism Technical Support Office (CTTSO)

US Department of State

US Embassy

Victoria Police