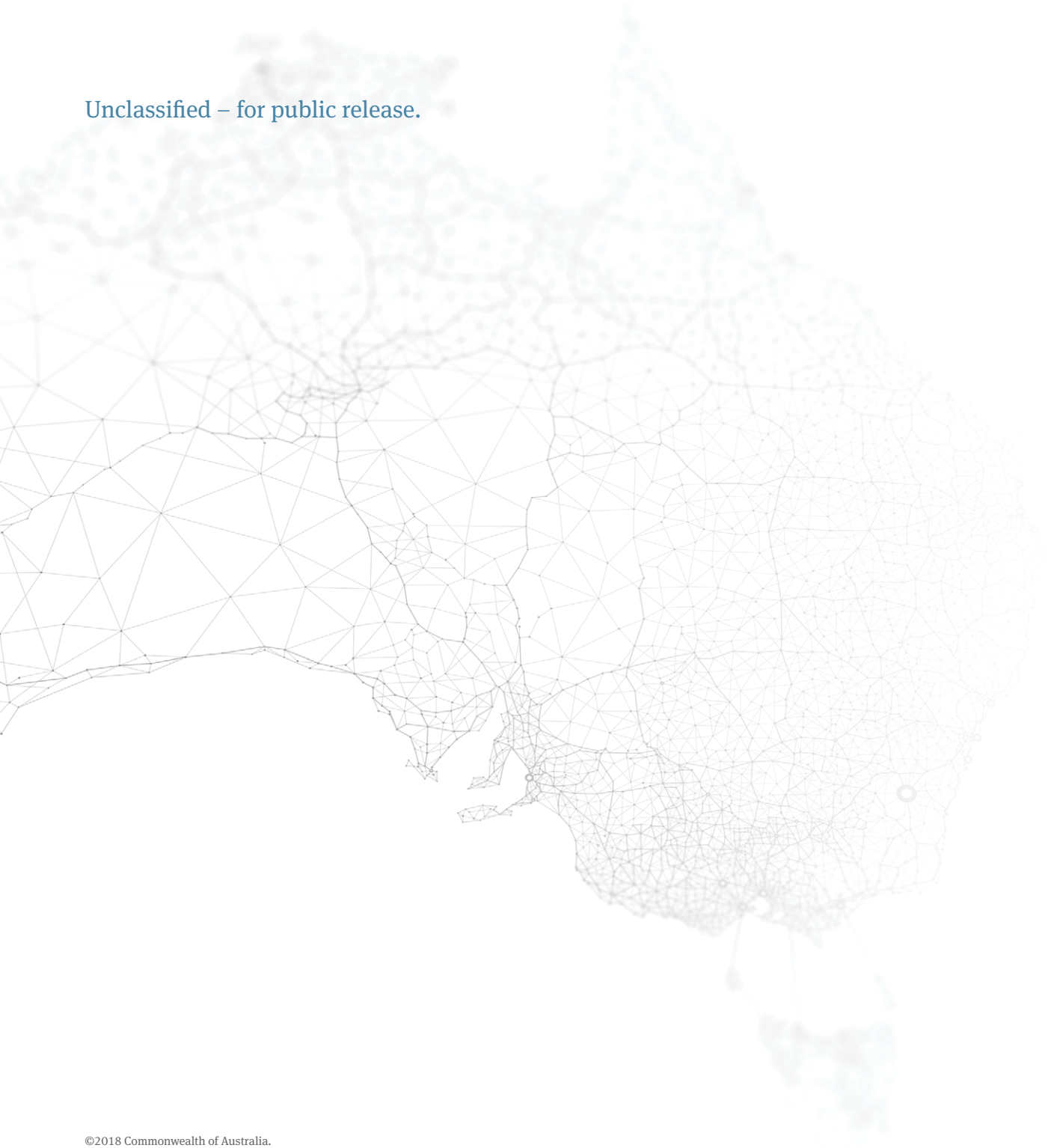
Australian Government

NATIONAL SECURITY SCIENCE AND TECHNOLOGY

Policy and priorities

Unclassified – for public release.



Defence Science and Technology
David Warren Building
24 Scherger Drive, Canberra Airport ACT 2609

nsstcexternal@dst.defence.gov.au
www.dst.defence.gov.au

AIM AND PURPOSE

Science and technology innovation plays a core role in our nation's security. As access to science and technological developments and ideas move from the realms of specialists in laboratories and on to the internet for public view, there is an increase in our nation's vulnerability to technology-based threats.

The National Security Science and Technology Centre (NSSTC) was created to help Australia's national security agencies collectively understand and prioritise their science and technology requirements, and to coordinate research and development to address these priorities by fostering partnerships between Australia's national security agencies and academics, industry and other potential science and technology providers.

The aim of this document is to outline Australia's current national security science and technology priorities and coordination of efforts, to best take advantage of investment in science and technology and address gaps in immediate and future national security capability.

POLICY CONTEXT

The Defence White Paper 2016 endorsed Defence Science and Technology's responsibility for leading and coordinating the delivery of science and technology to support national security agencies. DST has held a similar role in support of Defence for over 100 years. The NSSTC within DST is responsible for undertaking this function.

The Defence Industry Policy Statement also noted that Defence Innovation Forums will *"provide a venue for communicating national security science and innovation priorities."*

Recent policy reviews have further articulated the need to ensure that Australia's science and innovation capabilities are best utilised for our current and future national security capabilities. These include the recent review of the National Counter-Terrorism Plan[1] and the the 2017 Independent Intelligence Review (June 2017[2]). The Intelligence Review specifically recommended the establishment of a National Intelligence Community (NIC) Science and Technology Advisory Board, to provide a more structured response to technological change and the need to coordinate science and technology across the expanded NIC. The recommendations to establish a Joint Capability Fund and a forward looking Intelligence Capability Investment Plan also attest to the need for a more coordinated approach to capability development across the community.

In addition, the establishment of the Home Affairs portfolio and the Office of National Intelligence will ensure more enduring and better integrated intelligence and domestic security arrangements[3]. While this paper outlines the national security science and technology priorities, governance arrangements and engagement mechanisms as they exist now, these will need to co-evolve as arrangements are re-defined under the new national security architecture.

1. See https://www.nationalsecurity.gov.au/Media-and-publications/Publications/Documents/ANZCTC-National-Counter-Terrorism-Plan.pdf
2. See https://pmc.gov.au/resource-centre/national-security/report-2017-independent-intelligence-review
3. See https://www.pm.gov.au/media/strong-and-secure-australia

GOVERNANCE

A National Security Science and Technology Interdepartmental Committee (NSST IDC) was established in March 2017 to provide a cross-agency governance mechanism. This NSST IDC will review and endorse national security science and technology policies and priorities and promote cross-agency collaboration on science and technology, which will deliver efficiencies and reduce duplication.

The NSST IDC is co-chaired by Deputy Secretary National Security (Department of the Prime Minister and Cabinet) and the Chief Defence Scientist (Department of Defence), with senior members drawn from across Australian Border Protection, law enforcement, intelligence, Defence and policy agencies.

It is the role of the NSSTC to work with all agencies to collate and prioritise their national security science and technology priorities. NSSTC also works to ensure that these priorities reflect guidance from the Australia and New Zealand Counter Terrorism Committee (ANZCTC) and its subcommittees.

SCIENCE AND TECHNOLOGY PRIORITIES

As endorsed by the NSST IDC in March 2017, the current six national security science and technology priorities are the following:

- Cyber security
- Intelligence
- Border security and ID management
- Investigative support and forensic science
- Preparedness, protection, prevention and incident response
- Technology foresighting

These six priority themes are expanded in Annex A.

Given the changing nature of both the threat to Australia and the resulting science and technology challenges and opportunities, these statements of science and technology priorities will be reviewed and updated annually.

ENGAGEMENT MECHANISMS

NSSTC will assist national security agencies to elucidate their science and technology requirements, and then foster collaboration with the innovation community to address these requirements.

There are multiple engagement mechanisms that NSSTC uses to implement these two roles.

Government agencies

There are two key fora for high-level engagement across national security agencies for science and technology. These are:

1. The National Security Science and Technology Interdepartmental Committee (as described on page 2), providing an engagement mechanism across the key federal agencies. This Band 2/3 committee is supported by a Band 1 Roundtable with representation from the same agencies.
2. The ANZCTC and its sub-committees, providing a mechanism to engage the jurisdictions and first responder community.

In addition, two-way staff exchanges are encouraged between the national security agencies and the NSSTC. For example, the NSSTC includes a Science Counsellor role intended to function on a full or part-time basis within another agency.

NSSTC will also facilitate in-depth workshops on commonly identified science and technology themes. This brings users and technology experts together to discuss particular needs and then define a collaboratively-funded cross-agency program of research and development activities.

Industry, academia and other publically funded research agencies

An informed and engaged national security science and innovation community in Australia is key to driving the state of the art and delivering capability to the national security agencies. The NSSTC will create a *"National Security Science and Technology Research Forum"* to facilitate engagement with the national security innovation community. This Forum will outline research and development opportunities, bring together communities of interest for conferences or workshops, announce upcoming events and advertise other news.

Engagement with industry, publically funded research agencies, and academia will also be fostered via mechanisms such as the Innovation Portal managed by the Centre for Defence Innovation Capability, and through engagement with domain-specific hubs.

The Defence Innovation Portal is a website that links to the Defence Innovation Hub and the Next Generation Technologies Fund, allowing the innovation community access to opportunities in science and technology that address Defence-specific priorities. In line with the Defence Industry Policy Statement, the *"National Security Science and Technology Research Forum"* will be linked to this Portal.

International partners

In meeting the challenge of delivering the science and technology outcomes that are required, NSSTC will leverage the science and technology programs being undertaken internationally. The NSSTC has existing arrangements with the United States, Canada and the United Kingdom to share resources and collaborate on activities of mutual benefit, as follows:

- US Department of Homeland Security (Treaty arrangements)
- US Combating Terrorism Technical Support Office (MOU)
- Canadian Defence, Centre for Security Science (MOU)
- UK Home Office (MOU)

The NSSTC will establish additional arrangements with other nations, particularly within our South East Asian regional environment.

NSSTC will continue to work closely with the national security agencies to shape the science and technology programs pursued with our international partners.

TRANSLATION TO CAPABILITY

An informed and systematic identification of science and technology priorities and a research and development program to address these is an essential starting point to address gaps in capability. Eventually, this work is required to be translated into resourced programs of work to deliver actual capability.

Capability enablers

Science and technology alone will not produce or impact capability without technology transfer being undertaken collaboratively by the national security user community. There are a number of capability enablers which need to be identified and collective actions considered. Training is one such enabler, both to allow existing staff to be re-trained on new capabilities and new staff to become proficient with the capabilities they will be using. A collective approach to training on new capabilities with cross-agency applicability is more efficient than individual agencies undertaking their own bespoke training. Other capability enablers include ICT architectures, facilities, support/maintenance, workforce and integration with existing systems so that they are aligned and able to receive and utilise the science and technology support. While a discussion of all the capability enablers is beyond the scope of this document, they will need to be considered although their provision is not within the scope of the NSSTC's role.

Funding

Currently, many of the investments in science and technology that are being made across the national security community are by individual agencies with individual suppliers. The same is also true for the capability enablers discussed earlier. NSSTC's role is to raise collective awareness across the agencies of these investments, to potentially enable a more collective and efficient approach, and facilitate the pooling of resources across agencies who share common capability goals and requirements. The Government will expect agencies that have common interests to share, coordinate and leverage each other as much as possible. This approach also aligns well with the recommendations from the Intelligence Review, particularly those around a more collective approach to capability planning and investments across the National Intelligence Community.

BENEFITS OF A COORDINATED APPROACH TO SCIENCE AND TECHNOLOGY FOR NATIONAL SECURITY

The NSSTC will drive Australia's national security community to a more collaborative co-investment approach...

The NSSTC will drive Australia's National Security community to a more collaborative co-investment approach between government, academia and industry that effectively and efficiently delivers innovative science and technology solutions in the agreed priority areas. Maximising leverage internationally and building capability nationally, through engagement with industry, academia and publically funded research agencies will ensure Australia remains on the forefront of science and technology in order to remain agile and anticipative of new and emerging threats.

ANNEX A: SCIENCE AND TECHNOLOGY PRIORITIES

Cyber security

To anticipate vulnerabilities, strengthen cyber systems and critical infrastructure, and enhance national capacity to respond to and recover from cyber-attack, investment in science and technology is crucial to ensure we remain alert and responsive to evolving threats.

Many of the agencies consulted noted the need for research to support the continued and growing requirement for scalable high assurance, resilient computing for multilevel security, secure gateways allowing agencies to have connectivity between the internet facing elements of their role and the sensitive information held within the agencies, as well as secure cloud based storage. Secure communications, enabling agencies to undertake their mission successfully are also critical and were highlighted as a requirement by some agencies.

Other requirements highlighted in this priority area by a few of the agencies consulted include the need to develop science and technology programs to strengthen cyber systems to ensure our agencies remain alert and responsive to evolving threats.

Intelligence

Systems delivering timely and accurate information intelligence are critical for national security, not only for intelligence and law enforcement agencies but also border protection and health authorities. Rapidly changing and advancing technologies are transforming how information is collected, integrated and exploited. The ability to automate data fusion, data integration and data analysis is a common need across agencies and requires a coordinated effort. It is worth noting that these efforts would need to operate within current policy boundaries, ensuring that the privacy of Australians is met.

As highlighted by many of the agencies consulted, the information rich age brings with it a suite of new challenges. Common amongst many in the community is the enduring need for data analytics across a range of classifications including social media and open source exploitation. Many of the agencies noted the need for greater automation with some highlighting that this should occur as close to the point of collection as possible. Further to this, the systems and services enabling intelligence exploitation need to be trusted by the user, with high integrity and reliability, underpinned by a quality assurance framework. Critical supporting elements in this priority area were highlighted by some and include the specific requirement for data analytics including; image processing, speech and text language processing and physiological analysis.

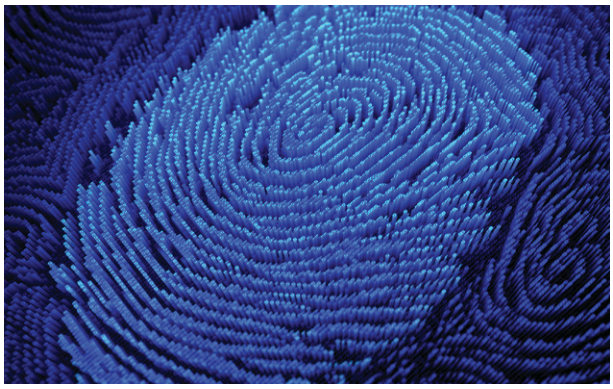
The need for smart buyer advice and access to other science and technology subject matter expertise was highlighted by some of the agencies. A few agencies highlighted the requirement for products to be machine readable.

Border security and identity management

Science and technology can enhance the capability to track and identify objects or people and monitor or screen for hazardous materials or threats. This can involve the observation and assessment of explosives, chemical, biological or radiological agents, disease, drugs and other contraband. In tracking objects, tools can detect and trace movement and authenticate identity.

The key theme to emerge in this priority area was the capability to identify objects. Many of the agencies consulted highlighted the continued need for science and technology to support development in biometrics broadly. This includes the need for the development of methods to enable both field deployable and scalable stand-off biometric capabilities. Challenges including the ability to compare biometric data from different quality data sets, as well as the need for secure real time linkages to internet facing capabilities (see Cyber Security) were identified as an important aspect of this challenge by some agencies. Many agencies also raised the requirement for the development multimodal biometric techniques. The requirement for the development of remote sensors to track things was raised by a few agencies.

A few agencies also had requirements for support to behaviour analysis.



Investigative support and forensic science

The ability to use information to deliver forensic and investigative support to our national security and law enforcement agencies is essential in ensuring effective prosecutions or the disruption of terrorist and trans-national criminal activities. New technologies are needed to enable the 'in-field' screening and analysis of items to provide timely, accurate, scientific information to support investigations.

Research programs advancing the state of the art in traditional forensic science and technology, including that related to fingerprints, genetic material, illicit drugs, explosives and other trace and physical evidence are ongoing in academic, industry and government facilities.

With the increase in the use of digital technologies some agencies identified a requirement for more advanced digital forensic tools to support investigations.

The forensic science community continues to enhance capabilities to detect, record, collect and analyse physical, biological and digital traces. There is a requirement to evolve these capabilities through research to ensure the capabilities are effective in the changing environment. Regardless of the change, the common goal is to answer the following questions in a timely and accurate manner: who, what, where, why, how and when.

The expanding role for forensic science and other technical capabilities in the national security environment sees these specialist capabilities at the centre of supporting community safety and security through disruption activities and also justice through traditional support to prosecutions. These capabilities are increasingly informing policy and capability enhancements through technical assessment of emerging threats. The relationship between intelligence and science is essential to ensure forensic science and other technical capabilities evolve to be agile to the threat in the dynamic operational environment and lead times for the operationalisation of new capabilities are minimised.

Preparedness, protection, prevention and incident response

Australian agencies need to be appropriately equipped and prepared to effectively and safely respond to events of national security significance. This requires a range of responses that span the Prepare – Prevent – Respond – Recover spectrum. This includes: physical resilience; social and cultural resilience; forecasting, modelling and risk assessment; first responder capabilities; and information management.

Not unexpectedly, this priority area covers the broadest range of topics. Important aspects identified by some of the agencies consulted within this priority include the enduring ability to prepare for, protect against, prevent and respond to CBRNE events with an emphasis on remote means. Recent events highlight the need for continued improvements in non-intrusive inspection techniques as well as explosive trace detection which were requirements for some agencies.

Science and technology to support activities to counter violent extremism was highlighted as a need by some agencies.

Methods and techniques to identify a threat from and to counter uncrewed aerial systems/vehicles is a common requirement, as well as using these uncrewed devices to provide tactical capabilities such as surveillance and communications.

Support to understand the requirements for critical infrastructure and physical resilience as well as the protection of crowded places were identified by some agencies, as was modelling support broadly. Plume and blast models, as well as tools to enable forecasting and risk assessment were highlighted as requirements by a few.

First responder capabilities, including requirements for secure communications on the move and power generation in remote locations were raised as important by a few agencies.

Technology foresighting

Australian agencies need to position themselves to minimise strategic surprise. Technology foresighting will monitor global technology trends and developments in emerging science to forecast future challenges and opportunities to achieve this goal.

DST has a cell which maintains a science and technology horizon scanning capability in partnership with international agencies. This horizon scanning provides a broad perspective on potential game-changing threats and opportunities.

Technologies which are identified as having potential for disruptive impact are then examined in more depth. Emerging and Disruptive Technologies Assessment Symposia (EDTAS) are now a biannual event co-hosted by DST, with the focus on a new ‘disruptive’ or ‘game changing’ technology at each event. Recent symposia have looked at the themes of Trusted Autonomous Systems and Digital Disruption. Future symposia will explore themes of advanced sensors, materials science/advanced manufacturing and quantum technologies.

We would welcome ideas from the science, technology and innovation community on possible future challenges and opportunities for national security science and technology.