National Intelligence Discovery Grants (NIDG) Program

ID25: Intelligence Challenges 2025

The *2017 Independent Intelligence Review* (IIR) identified a number of challenges facing Australia's intelligence enterprise over the coming decade. These included the increasing complexity of the geostrategic environment, broadening scope of national security and intelligence missions, rapid pace of scientific and technological change and high levels of innovation investment by other nations. To meet these challenges the Review recommended, among a number of other recommendations, a more systematic approach to leveraging science and technology.

To enable the National Intelligence Community (NIC) to better leverage emerging science and technology, the following nine challenges have been identified as being the priority areas for the *National Intelligence Discovery Grants* (NIDG) Program (ID25) for funding commencing in 2025.

1. Covert collection challenges

The ability to access and collect intelligence from people, imagery, signals, or emanations, signatures, nodes, networks (including internet-of-things environments) and transactions with a low probability of detection and/or attribution. The ability to degrade or defeat adversary collection and cyber capabilities to safely move people, information and equipment into, out of, and through environments with low signature and likelihood of detection and/or attribution.

Examples of research fields include:

- Sensors, signatures, signals, emanations and networks.
- Forensic methods to detect and analyse tampering or manipulation of satellite imagery and other remote sensing data.
- Computer network exploitation.
- Covert, secure and assured communications and internet traffic including attribution and decloaking or otherwise anonymised traffic (e.g. I2P).
- Financial intelligence including cryptocurrency, block-chain and distributed ledger technologies.
- Emerging encryption technology including homomorphic and quantum based.

2. Space-based challenges

The ability to leverage low cost and innovative technological advancement in space-based and high-altitude capabilities in a timely manner to improve collection, communication and analysis capabilities.

Examples of research fields include:

- Satellite communications, sensors and networks.
- Automation and on-board processing and analysis.
- Advanced materials.
- Space-based situation awareness.
- Counter space-denial capabilities.

3. Identity management challenges

The ability to quickly, accurately and uniquely identify individuals from all types of data (online, surveillance, biometric, speech, behavioural, forensic, text, etc.), including where the data has low linkages to real world identities. The ability to mask or obfuscate the identity of an individual from adversaries where access to online, surveillance, biometric, forensic or other data is available.

Examples of research fields include:

- Biometrics, biological or behavioural (e.g. gait analysis) for authentication, biometric authentication mechanisms and counter biometric considerations.
- Bio- and geo- forensics (including for law enforcement and prosecutions).
- Deep fakes/synthetic content analysis and detection
- Deep fake counter-measures and considerations (e.g. that defeat traditional security measures).
- Web-scraping and machine learning for identity data.
- Socio-technical systems and systems integration.
- Named entity recognition using probabilistic methods.
- Identity verification processes for financial intelligence.
- Awareness and management of consumer data collection.

4. Emerging biological science challenges

The ability to develop methodologies, techniques, services and devices from emerging biological technologies to provide new or alternate options to meet existing and future intelligence mission objectives. The ability to detect, identify, analyse, counter, defeat and prosecute threats from emerging biological technologies, in a safe and timely manner. The ability to exploit advances in machine learning to enable the above.

Examples of research fields include:

- Emerging biotechnology (e.g. in molecular biology, chemical sciences).
- Synthetic biology (e.g. genetic engineering, emerging threats, ethical, legal and societal aspects).
- Immunology and microbiology (e.g. emerging threats and applications).
- Pathogen threat detection and modelling.
- Human augmentation technologies (e.g. neuroscience advancements, human-machine interface and wearable devices).

5. Emerging material science challenges

The ability to develop methodologies, techniques, services and devices from emerging material technologies to provide new or alternate options to meet existing and future intelligence mission objectives. Identification, development and employment of new or novel materials with unique properties, including rare earths and complex alloys, to gain technical, performance and cost benefits. The ability to exploit advances in machine learning to enable the above.

Examples of research fields include:

- Nanotechnology and material science (e.g. miniaturisation and new functions).
- Emerging semi-conductor and related technologies.
- Convergence or integration of technologies (e.g. nano-, bio- and info- technologies).
- Human augmentation technologies, human-machine interface and wearable devices.

- Quantum sensing and supporting technologies.
- Quantum material science and engineering related computing.

6. Cyber security, protective security and offensive cyber challenges

The ability to ensure the security and integrity of sensitive and classified information whilst enabling flexible/remote working and crisis response. The ability to predict, prevent, detect, attribute, respond and recover from cyber incidents and malign online interference (foreign, domestic, insider) at a national scale. The ability to conduct offensive cyber and informational activities to disrupt emerging security threats.

Examples of research fields include:

- Cyber (and national infrastructure) systems analysis, vulnerability, risk, resilience.
- Human aspects of cyber security (e.g. insider threat, behavioural analysis, sentiment analysis).
- Mobile device trust/assurance for remote access and collaborative working.
- Networking and sensor technologies including internet-of-things (e.g. LoRaWAN or related technology).
- Supply chain security/intelligence.
- Blockchain intelligence. Insight into emerging digital currency management tools.
- Cryptography including crypt architecture and crypt engineering/implementation.
- Crypto-jacking prevention and forensic science.
- Side channel analysis.
- Novel models for achieving rapid high assurance certification, accreditation, and deployment of technologies for high secure networks and systems.
- Quantum technologies and supporting technologies.
- Cyber extortion (e.g. ransomware) response and countermeasures.
- Emerging technologies in creating deficiencies or augmenting existing practices.
- Dual design to incorporate both security/privacy and lawful access.
- Integration of AI with computer network exploitation and computer network defence.

7. Human behaviour and influence challenges

The ability to identify and understand actors' psychologies, social identities, narratives and behaviours that constitute a threat to Australia's security. The ability to mitigate and counter the cultural, psycho-social and organisational drivers and antecedents to national security threats. The ability to influence target audiences to elicit information, affect behaviour or shape preferences.

Examples of research fields include:

- Network analysis and disruption techniques (e.g. criminal, terrorist, etc.).
- Behavioural analysis (e.g. NLP and language agnostic) of individuals and groups, including in person, online and via multi-source digital data sets to profile and predict psychological phenomena (e.g., motivation, intent, loyalty, trust).
- Building trust and influence and eliciting information, including influencing outcomes in cross-cultural, hostile, resistant, conversational and time-sensitive contexts (in person and online).
- Identifying and countering malign interference, influence and disinformation.
- Identifying drivers, antecedents and pathways to radicalisation and extremism.

- Understanding actors, communities, cultures, identities and narratives and influencing effects / outcomes.
- Identifying trends in transnational, serious and organised criminal activities.
- Detecting and countering adverse 'crowd' or mass behaviour.
- Human vulnerabilities related to cyber-extortion, trafficking, bribery and corruption.
- Elicitation and credibility assessment.
- Resilience and functioning when alone/remote in oppressive or extreme environments.
- How deep or strategic fakes influence decision making and/or disrupt social norms.

8. Data-driven and real-time analytical challenges

The ability to employ advanced machine learning, natural language technologies and data science techniques to autonomously (or semi-autonomously) identify, extract, fuse and disseminate meaningful intelligence from large, disparate, sparse and/or incomplete data sets, including linguistic (text, speech, etc.), geospatial, financial, signals, identity and other relevant data sets. The ability to do this at the speed and scale required to meet emerging threats.

Examples of research fields include:

- Data management, data engineering and data curation.
- High performance computing.
- Automated information fusion, filtering, triage and knowledge management.
- Advanced sampling, pattern recognition, predictive analytics and statistics.
- Natural language processing, large language models and other language technologies.
- Financial intelligence analytics using large language models.
- Deep learning for large and disparate data sets.
- Human-systems integration and uncertainty analysis.
- Ethical, legal and societal aspects of AI (e.g. trust, bias, discrimination, privacy, etc.).
- Techniques to account for human factors (e.g., errors, biases) in the interpretation and use of data.
- Quantum Information Sciences, including quantum algorithm development, testing and costing.
- Emerging ubiquitous technical surveillance technologies and dynamics.

9. Situation awareness and multi-source assessment challenges

The ability to analyse and assess significant events and trends that impact on Australia's national security and interests (including political, strategic, environmental and economic developments as well as trends in adversarial behaviour, capability or investment in S&T). The ability to collaboratively analyse and synthesise evidence from multiple sources, and across multiple agencies, to produce timely, high quality and influential intelligence reports and assessments. The ability to articulate the basis and level of confidence in assessments.

Examples of research fields include:

- All-source intelligence integration and collaboration technologies.
- Political, strategic, economic and 'drivers of conflict' research and analysis including overt and covert propaganda and influence campaigns.
- Technology forecasting: emerging, critical and disruptive technologies including deficiencies and/or strengths in Australian capabilities (e.g. Quantum and AI).

- National Security implications of environmental change (e.g. forecasting certain climate change impacts) and health crises (e.g. epidemic, pandemic and agricultural impacts).
- Risk and resilience frameworks and measurements for security threats.
- Understanding and avoiding bias (e.g. algorithmic bias) and generating confidence measures for assessments.
- Enhancing cognition, comprehension, memory, learning and decision-making formally and in-the-field (e.g. visualisation).
- Detection of nefarious crowdsource fundraising.
- Identifying fundraising under false pretext to fund illicit activities.
- Emerging technology enabled fraudulent international transaction monitoring.
- The application of threat modelling and development of tools and strategies for cyber security resilience and information assurance.