National Intelligence and Security Discovery Research Grants Program

Round 3 (2023): Intelligence Challenges

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 to better leverage emerging science and technology the following eight challenges have been identified as being the priority areas for engagement with the research and innovation sectors.

Science and Technology Challenges

1. Covert collection challenges

The ability to access and collect intelligence from people, imagery, signals, signatures, nodes, networks (including internet-of-things environments) and transactions with a low probability of detection and/or attribution. The ability to 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 science and technology research include:

- Access technologies
- Imagery and geospatial intelligence
- Sensors, signatures, signals and networks
- Computer network exploitation
- Covert, secure and assured communications
- Financial intelligence; and
- Cryptocurrency, block-chain and distributed ledger technologies.

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 science and technology research include:

- Launch technologies
- Mission control systems and systems integration
- Satellite communications, sensors and networks
- Automation and on-board processing and analysis
- Advanced materials
- Space-based situation awareness; and
- 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 science and technology research include:

- Biometrics (including behavioural biometrics)
- Deep fakes and generative adversarial networks (GAN)
- Bio- and geo- forensics (including for law enforcement and prosecutions)
- DNA / RNA
- Web-scraping and machine learning for identity data
- Counter biometric surveillance; and
- Socio-technical systems and systems integration.

4. Emerging biological and material science exploitation challenges

The ability to develop methodologies, techniques, services and devices from emerging biological, material and other 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 technologies, in a safe and timely manner. The ability to exploit advances in machine learning to enable the above.

Examples of science and technology research include:

- Biotech engineering (e.g. CRISPR), synthetic biology (e.g. data storage)
- Immunology and microbiology (e.g. gene sequencing and applications)
- Nanotechnology and material science (e.g. miniaturisation and new functions)
- Convergence or integration of technologies (e.g. nano-, bio- and info- technologies)
- Human augmentation technologies, human-machine interface and wearable devices; and
- Threat detection and remediation (e.g. explosives, radiological and pathogens).

5. 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 science and technology research include:

- Cyber (and national infrastructure) systems analysis, vulnerability, risk, resilience
- Human aspects of cyber security (e.g. insider threat, behavioural analysis)
- Mobile device trust/assurance for remote and collaborative working
- Secure data transport
- Networking and sensor technologies (including internet-of-things)
- Supply chain security/intelligence
- Cryptography, quantum technologies and photonics; and
- Automated at-scale response.

6. 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 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 science and technology research include:

- Network analysis and disruption techniques (criminal, terrorist, etc.)
- Analysing online behaviour and profiling individuals and groups
- Building trust, rapport and influence and eliciting information
- 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; and
- Influencing 'crowd' or mass behaviour.

7. 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 science and technology research include:

- Data management, data engineering and data curation
- Automated information fusion, filtering, triage and knowledge management
- Advanced sampling, pattern recognition, predictive analytics and statistics
- Natural language processing and other language technologies
- Deep learning for large and disparate data sets
- Human-systems integration and uncertainty analysis; and
- Ethical, legal and societal aspects of AI/ML (trust, bias, discrimination, privacy, etc.).

8. 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 science and technology research include:

- All-source intelligence integration and collaboration technologies
- Political, strategic, economic and 'drivers of conflict' research and analysis
- Advance 'red-teaming', 'war-gaming', scenarios and course of action analysis
- Technology forecasting: emerging, critical and disruptive technologies
- Security implications of environmental change and health crises
- Risk and resilience frameworks and measurements for security threats
- Understanding and avoiding bias (e.g. algorithmic bias) and generating confidence measures for assessments; and
- Enhancing cognition, comprehension, learning and decision-making (e.g. visualisation, etc.).