Australian Government | NIC National Intelligence Community

National Intelligence Explore Award
Intelligence Science and Technology Challenges 2026-27

The 2017 Independent Intelligence Review and 2024 Independent Intelligence Review emphasised the importance of strong, systematic partnerships to the National Intelligence Community's (NIC) ability to meet current challenges and prepare for future challenges. As Australia's R&D ecosystem can support the NIC's future operating environment, there is scope to give more substance to the NIC's partnerships with the private sector and research institutions. It is recommended to review the **2024 Independent Intelligence Review**, particularly Chapter 13 (Technology). The following ten Challenges have been detailed to inform research proposals to the NIC Research program to leverage emerging science, technology and social science, for funding commencing in 2027.

Covert collection challenges

The ability to:

- Access and collect intelligence from people, imagery, signals, emanations, signatures, nodes, networks and transactions with a low probability of detection and/or attribution.
- 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.
- Operate with respect to ethical, social and regulatory (e.g. legislation, treaties, conventions) standards and considerations.

Research opportunities may include (but are not limited to):

- Sensors (quantum, classical), signatures, signals analysis, emanations and networks.
- Forensic methods to detect and analyse tampering or manipulation of data.
- Covert, secure and assured communications and internet traffic including encryption, attribution and decloaking or otherwise anonymised traffic.
- Financial intelligence including cryptocurrency, block-chain and distributed ledger technologies.
- Emerging encryption technology including homomorphic and quantum based.

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.
- Mask or obfuscate the identity of an individual from adversaries where access to online, surveillance, biometric, forensic or other data is available.
- Operate with respect to ethical, social and regulatory (e.g. legislation, treaties, conventions) standards and considerations.

Research opportunities may include (but are not limited to):

- Biometrics, biological or behavioural for authentication, entity resolution, identity verification and counter biometric considerations.
- Bio- and geo- forensics (including for law enforcement and prosecutions).
- Deep fakes/synthetic content analysis, detection and countermeasures.
- Identity monitoring processes for financial intelligence.

FOI: This is an exempt document under the *Freedom of Information Act 1982*. It must be handled in accordance with the *Office of National Intelligence Act 2018* and the Protective Security Policy Framework.

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.
- Detect, identify, analyse, counter, defeat and prosecute threats from emerging biological technologies which have the potential to cause harm or detrimentally impact other organisms, materials, or infrastructure.
- Operate with respect to ethical, social and regulatory (e.g. legislation, treaties, conventions) standards and considerations.

Research opportunities may include (but are not limited to):

- Emerging biotechnology applications (e.g. synthetic biology, quantum biotechnology, bio-based computing and data storage, biohybrid materials (e.g. electronics, sensors etc) and bioenergy).
- Convergence of AI tools and emerging biological science.
- Pathogen threat detection, surveillance, modelling and intelligence.
- Human augmentation technologies (e.g. neuroscience advancements, human-machine interface and wearable devices).
- New/novel forecasting techniques to enhance intelligence and national security (e.g. health, environment, CBRN).

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.
- Identify, develop and/or employ new or novel materials with unique properties, including rare earths and complex alloys, to gain technical, performance and cost benefits.
- Operate with respect to ethical, social and regulatory (e.g. legislation, treaties, conventions) standards and considerations.

Research opportunities may include (but are not limited to):

- Semi-conductor, power sources, batteries and related technologies.
- Precision manufacturing.
- Convergence or integration of technologies (e.g. nano-, bio- and info- technologies).
- Human augmentation technologies (e.g. human-machine interface and wearable devices).
- Quantum sensing and supporting technologies.

Extreme environment challenges

The ability to:

- Leverage low cost and innovative technological advancement for future applications in extreme environments (e.g. space-based, high-altitude, ocean and undersea) capabilities in a timely manner to improve collection, communication and analysis capabilities.
- Operate in extreme environments.
- Operate with respect to ethical, social and regulatory (e.g. legislation, treaties, conventions) standards and considerations.

Research opportunities may include (but are not limited to):

- Communications, sensors and networks.
- Advanced materials, power sources, batteries and related technologies.
- Space-based situational awareness (e.g. satellite imagery and communications)
- Personnel resilience and function in oppressive, burdensome or extreme environments.

FOI: This is an exempt document under the *Freedom of Information Act 1982*. It must be handled in accordance with the *Office of National Intelligence Act 2018* and the Protective Security Policy Framework.

Emerging data science challenges

The ability to:

- Develop and apply advanced computational approaches to meet existing and future intelligence mission objectives (e.g. post-quantum compute).
- Employ advanced data science techniques and AI / ML modelling to autonomously (or semi-autonomously) identify, extract, fuse and disseminate meaningful intelligence from large, disparate, sparse and/or incomplete data (e.g. linguistic, geospatial, financial, signals, identity) at the speed and scale required to meet emerging threats.
- Operate with respect to ethical, social and regulatory (e.g. legislation, treaties, conventions) standards and considerations.

Research opportunities may include (but are not limited to):

- Data management, data security, data assurance, data engineering and data curation.
- Automated information fusion, filtering, triage and knowledge management.
- Advanced technical surveillance, sampling, pattern recognition, predictive analytics, language processing and statistics.
- Emerging financial intelligence analytics.
- Human-systems integration and uncertainty analysis.
- Quantum information sciences, including quantum algorithm development and post-quantum computing techniques.

Cyber security, protective security and physical security challenges

The ability to:

- Ensure the security and integrity of sensitive and classified information through the hardening of physical, information, personnel and cyber security practices.
- Predict, prevent, detect, attribute, respond and recover from major incidents and malign online interference (foreign, domestic) at a national scale.
- Conduct cyber and informational activities to disrupt emerging security threats.
- Proactively detect and respond to insider threat behaviours of concern.
- Operate with respect to ethical, social and regulatory (e.g. legislation, treaties, conventions) standards and considerations.

Research opportunities may include (but are not limited to):

- Cyber and national infrastructure systems analysis, vulnerability, risk and resilience, including mobile devices, remote access, networking and sensor technologies.
- Human aspects of cyber security (e.g. behavioural analysis, sentiment analysis, insider threat detection, societal existential risks).
- Understanding and defence against frontier AI/ML capabilities that autonomously identify and exploit complex software vulnerabilities.
- Supply chain integrity, verification, optimisation and security (e.g. blockchain intelligence and insight into emerging digital currency management tools).
- Cryptography including crypt architecture, crypt engineering/implementation and side channel analysis and crypto-jacking prevention.
- Novel models for achieving rapid high assurance certification, accreditation and deployment of technologies for high secure networks, systems and facilities.
- Emerging quantum technologies to support security practices.
- Cyber extortion (e.g. ransomware, scams) response and countermeasures.

FOI: This is an exempt document under the *Freedom of Information Act 1982*. It must be handled in accordance with the *Office of National Intelligence Act 2018* and the Protective Security Policy Framework.

Situational 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, economic, CBRN, adversarial behaviour, capability or investment in science, technology and social science).
- Collaboratively analyse and synthesise complex evidence from multiple sources, and across multiple agencies, to produce timely, high quality and influential intelligence reports and assessments.
- Operate with respect to ethical, social and regulatory (e.g. legislation, treaties, conventions) standards and considerations.

Research opportunities may include (but are not limited to):

- 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.
- New/novel technology forecasting for emerging, critical and disruptive technologies to enhance intelligence and national security (e.g. geospatial, geopolitical, health, CBRN, financial) including deficiencies and/or strengths in Australian capabilities.
- National security implications of environmental change (e.g. forecasting climate change impacts) and health crises (e.g. epidemic, pandemic and agricultural impacts).
- Enhancing cognition, comprehension, memory, learning and decision-making formally and in-the-field.
- Identifying fundraising under false pretext to fund illicit activities (e.g. nefarious crowdsource fundraising).
- Situational awareness in extreme environments.

FOI: This is an exempt document under the *Freedom of Information Act 1982*. It must be handled in accordance with the *Office of National Intelligence Act 2018* and the Protective Security Policy Framework.

Social behavioural challenges

The ability to understand human behaviours in social context. The prime focus is to understand human behaviour, cognition and social structure to:

- Identify and understand actors and bystanders' psychologies, social identities, narratives and behaviours that constitute a threat to Australia's security.
- Mitigate and counter the cultural, psycho-social, organisational and identity-based drivers and antecedents to national security threats.
- Influence target audiences to elicit information, affect behaviour or shape preferences.
- Understand the evolving nature of risk (insider and general) in the light of changing social and cultural norms and the evolving risk landscape.
- Operate with respect to ethical, social and regulatory (e.g. legislation, treaties, conventions) standards and considerations.

Research opportunities may include (but are not limited to):

- Identifying and countering malign foreign and/or domestic interference, influence and disinformation (including deep and strategic fakes).
- Identifying and/or understanding drivers, antecedents, pathways and barriers to radicalisation and extremism. Investigating what builds, maintains and threatens democratic support and social cohesion (e.g., understanding history, public imagination, language, culture) in multi-cultural and ethnic communities.
- Behavioural analysis to understand actors, communities, cultures, identities and narratives, motivators and goals, risk indicators, influencing effects/outcomes, and predict psychological phenomena (e.g. how individuals, groups and communities experience disinformation and polarisation, datafied society, insider risk).
- Building trust and influence and eliciting information, including influencing outcomes in cross-cultural, hostile, resistant, conversational and time-sensitive contexts (in person and online), elicitation and credibility assessments.
- Resilience and functioning when alone/remote in oppressive or extreme environments.

FOI: This is an exempt document under the *Freedom of Information Act 1982*. It must be handled in accordance with the *Office of National Intelligence Act 2018* and the Protective Security Policy Framework.

Socio-technical system challenges

The ability to understand how human behaviour and technical systems interact and shape one another. The prime focus is on how human and technological systems come together to:

- Identify and understand local and global (including transnational, serious and organised) threats to Australia's national security as related to the intersection and synthesis of humans, organisations and technological structures.
- Map, model and understand the emerging global and local social, political, cultural, ethical, scientific and technological institutions, infrastructure and environments within which contemporary and future security issues manifest.
- Model, including using AI and ML, complex (human and machine) behaviours at the intersection of institutional and technological change.
- Understand how technologies, institutions and publics have and do co-produce security and/or threat outcomes, de-/escalate scale and effect, and identify mitigation or extirpation opportunities.
- Operate with respect to ethical, social and regulatory (e.g. legislation, treaties, conventions) standards and considerations.

Research opportunities may include (but are not limited to):

- Mapping and understanding the impact of technological and organisational tools and infrastructures and of AI, ML and automation on bias, transparency and human decision making and behaviours.
- Investigating downstream effects on tech economy, organisations and products that result from individual and collective behaviours in complex systems, and vice versa.
- Understanding how deep or strategic fakes influence decision making and/or disrupt social norms.
- Understanding digital platforms, cyber operations and critical infrastructure as socio-technical spaces of national security significance and focus.
- Understanding generational human vulnerabilities related to developments in transnational, serious and organised cyber-extortion, trafficking, bribery and corruption.
- Examining laws, political and social pressures and global forces shaping critical technology research and development, and uptake and endorsement options and decisions. For example, this may include the evolution of democracy, human rights, privacy, civil liberties, freedoms, and rule of law within globalised big data/surveillance information ecosystems.
- Understanding how technological developments and products are designed, governed, used, resisted, imagined and experienced by humans.

FOI: This is an exempt document under the *Freedom of Information Act 1982*. It must be handled in accordance with the *Office of National Intelligence Act 2018* and the Protective Security Policy Framework.