Australia
India
Joint
Technology
Impact
Assessment
Project

Technology Impact Assessment for Peace and Stability:

Diplomatic Opportunities for Australia and India

2025

This project is funded by the Australia India Cyber and Critical Technologies Partnership

Project Overview

On 5 November 2024, Australia's Foreign Minister Senator Penny Wong announced in a joint press statement with the Indian Minister for External Affairs S Jaishankar that the Australian National University (ANU) had been awarded a grant to lead a project under the Australia India Cyber and Critical Technologies Partnership (AICCTP). Co-leader of the grant is InKlude Labs in Bengaluru. Researchers involved in the work also come from the Takshashila Institution, Social Cyber Institute, Arizona State University, Southern Cross University, Blended Learning International and RMIT University.

This project promotes rigorous ethical approaches to technology assessments of critical emerging technologies that impact peace and stability. It seeks to strengthen consensus among key stakeholders in Australia and India regarding the importance of a process for technology assessments that can be undertaken jointly with each other. Such activity would represent an important diplomatic innovation in bilateral relations for addressing the challenges posed by rapid technological advances and the evolving geopolitical landscape. The project aims to create a self-organising community of practice (CoP) inclusive of both countries, promoting its sustainability after the project's conclusion and potentially extending its influence on a wider multilateral scale.

To support these goals, the project will create an open-access curriculum for the professional education of government officials and stakeholders responsible for assessing critical and emerging technologies. Delivered over a year, the project is led by a multi-disciplinary team of senior researchers and professional educators from Australia and India who have expertise in technology, industry, economics, geopolitics, and public policy. This initiative is funded by the Australian Department of Foreign Affairs and Trade (DFAT) as part of the Australia India Cyber and Critical Technologies Partnership (AICCTP). For more information, videos and written product, see https://www.socialcyber.co/australia-india-tech-assessments.

Acknowledgements

The authors would like to acknowledge the contribution by speakers in our webinars and workshops, and by participants in our stakeholder interviews. We also recognise the role of more than 100 participants in our webinars and the workshop devoted to the topic of this paper. Pranay Kotasthane played an important role as advisor on the paper and the project. The team would also like to thank James Chapman and Zara Yap for administrative and technical support during the project; and Pranav Rao Bappanad for graphic design support through https://www.artstation.com/onedudecomics.

Australia
India
Joint
Technology
Impact
Assessment
Project

Technology Impact Assessment for Peace and Stability:

Diplomatic Opportunities for Australia and India

2025

Greg Austin
Karthik Bappanad
Adam Henry
Katina Michael
Lisa Materano
Bharath Reddy
Brendan Walker-Munro
Glenn Withers

This project is funded by the Australia India Cyber and Critical Technologies Partnership

Executive Summary

Australia and India have accumulated considerable good will and substantial experience of collaboration in science and technology that might now be turned more consistently to shared interests in peace and stability. Technology impact assessment (TIA) has been an essential diplomatic tool supporting international peace and stability since the late 1960s and 1970s, mostly through arms control treaties and international organisations specifically requiring such activities. Since that time, the number of cross-border or joint TIAs in various fields has markedly increased.

Throughout 1999, Russia and the United States (US), along with other countries, collaborated closely on assessments of control systems to protect against a nuclear command and control crisis from the Y2K challenge. By 2002, the United Nations (UN) was convening groups of experts to analyse the security implications of information and communications technologies. By 2022, the COVID pandemic had driven international TIA in the health sector very firmly into the realm of international stability as states struggled to shore up the economic and social foundations of economic security.

All the while, international standard-setting based on shared and debated technology assessments affecting security was being undertaken in a variety of multilateral regimes, such as the International Telecommunication Union (ITU) and the International Civil Aviation Organisation (ICAO). In the private sector, the Institute of Electrical and Electronics Engineers (IEEE) had become one of the most influential international actors in building bridges across geopolitical divides in global TIA practices, albeit on a limited scale and more in exchange and discussion than in advanced joint TIAs. By 2025, joint TIAs for peace and stability of one kind or another were being supported by diverse and numerous communities of practice.

The concept of joint technology impact assessment (TIA) had little purchase in the bilateral relationship between Australia and India until 2020. In July 2025, the two countries announced their first-ever inter-governmental joint assessment process in a field directly impacting peace and stability, namely undersea surveillance using several critical technologies.

Our research, published in an earlier research paper in this project, found that to the present day, neither country has institutionalised in its domestic policies a consistent framework for public-facing, open-access TIAs on issues influencing peace and stability. Both Australia and India have institutionalised the TIA process in public health and environmental policy, with varying degrees of public consultation and parliamentary oversight. However, neither country applies these processes of public consultation to matters of peace and stability on a consistent basis. The twin foundations of advanced TIA at the domestic level – public consultation and parliamentary oversight – are often less robust when applied to international issues.

Our previous paper compared the settings in each country for TIA of critical technologies affecting peace and stability. In the current paper, we analyse the arguments for why the two governments should establish a standing mechanism for bilateral TIA of critical technologies for that purpose. The mechanism would not need to be too formal or too structured, but it would need to recognise the key criteria for advanced TIA identified in both papers. It could be based on the concept of a community of practice for specialists, officials, and other stakeholders committed to and trained in TIA. There should be a governmental office responsible for guiding methodologies of technology assessment. This would have to be part of a more deliberate institutional redesign in bilateral security and science diplomacy, by both governments, to make joint TIA a much higher priority.

We identify four factors critical for success in future joint TIA between Australia and India: (1) political commitment; (2) institutional capacity; (3) resource allocation; and (4) cultural sensitivity. Geopolitical concerns will also come into play in shaping the choices for a particular TIA to be undertaken. Important technologies and areas of scientific research may remain off limits to bilateral activity because of such sensitivities. However, as existing joint programs demonstrate, there is a vast array of sub-fields that will not face such sensitivity. We mention three possible examples: (1) digital identity; (2) biotech for pathogen detection; and (3) maritime situational awareness.

At the same time, we suggest that efforts by Australia and India to promote TIA for peace and stability would reap greater diplomatic gains if they were framed as part of a campaign for a multilateral regime of TIA that is based on open communities of practice. These cross-border communities would involve trusted governments, community and business stakeholders, and specialists. Initiatives to develop a community of practice for TIA in peace and stability could be supplemented through the delivery of professional education in this field relying in part on a syllabus developed by this project. No country has the resources to independently undertake advanced TIA for all of the applications of critical and emerging technologies.

For Australia and India, this effort would focus on a political geography of shared interest, such as developing countries of the Indian Ocean region, Southeast Asia and potentially the South Pacific. This undertaking would ideally be based on a limited set of critical technologies of most value to those countries, such as artificial intelligence (AI) applications, for the purposes of economic development that is an essential underpinning regional security.

The idea of "TIA of critical technologies" might usefully become more prominent in the foreign policy and science diplomacy of Australia and India. OECD researchers in 2023 called out the value of a multinational hub for TA; and UN agencies in 2024 and 2025 made similar calls. In June 2025, the Sixth European Technology Assessment Conference (ETAC6) helped set the stage for this: it was dedicated to the theme of "Technology Assessment Goes Global" and was the first global convening of Technology Assessment (TA) practitioners and scholars.

Our proposition is to shift the locus of advanced TIA from Europe and the US, where it has been firmly established through four decades, to a gradually expanding number of geographies outside the club of advanced economies. Now that this globalisation of TIA has been launched, Australia and India have a unique opportunity to work collaboratively to shape this process while registering gains for their own national and bilateral interests in peace and stability.

Contents

List of Acronyms

3GPP	Third Generation Partnership Project
ABOC	Australian Border Operations Centre
AGARD	Advisory Group for Aerospace Research and Development
AGI	Artificial general intelligence
AI	Artificial intelligence
AICCTP	Australia India Cyber and Critical Technologies Partnership
AIO	Artificial intelligence optimisation
AIS	Automatic identification systems
AISA	Australian Information Security Association
AISRF	Australia India Strategic Research Fund
ANU	Australian National University
ARPANSA	Australian Radiation Protection and Nuclear Safety Agency
ASEAN	Association of Southeast Asian Nations
ASM	Advanced Semiconductor Materials
ASML	ASM Lithography
AU	African Union
AUDREY	Assistant for Understanding Data through Reasoning, Extraction and Synthesis
AUKUS	Australia, United Kingdom, United States
BRICS	Brazil, Russia, India, China, South Africa
BWC	Biological Weapons Convention
CCMS	Committee on the Challenges of Modern Society
CCST	Cabinet Committee on Science and Technology
CCW	Certain Conventional Weapons
CIA	Central Intelligence Agency
CISA	Cybersecurity and Infrastructure Security Agency
CISS	Centre for International Security and Strategy
CoP	community of practice
CRISPR	Clustered Regularly Interspaced Short Palindromic Repeats
CSET	Center for Security and Emerging Technology
CSIR	Council of Scientific and Industrial Research
CSIRO	Commonwealth Scientific and Industrial Research Organisation
CSP	Comprehensive Strategic Partnership
CT	Core Network and Terminals
CTBT	Comprehensive Nuclear Test Ban Treaty
CWC	Chemical Weapons Convention
DFAT	Department of Foreign Affairs and Trade
DHS	Department of Homeland Security
DISR	Department of Industry, Science and Resources
DNA	Deoxyribonucleic acid
DPI	Digital Public Infrastructure
DPTs	Defence Policy Talks
DRDO	Defence Research and Development Organisation
DSCI	Data Security Council of India
DSTG	Defence Science and Technology Group
DTA	Digital Transformation Agency
EC	European Commission
EEZ	Exclusive economic zone
EP	European Parliament
EPRS	European Parliamentary Research Service
ETAC6	European Technology Assessment Conference, Sixth
EU	European Union
EuroQCI	European Quantum Communication Infrastructure

GGE	Group of Governmental Experts
GPAI	Global Partnership on Artificial Intelligence
GPS	Global Positioning System
HALE	High-Altitude Long Endurance
IAEA	International Atomic Energy Agency
ICAO	International Civil Aviation Organisation
ICBM	Intercontinental ballistic missile
ICT	Information and communications technologies
IEEE	Institute of Electrical and Electronics Engineers
IFC-IOR	Information Fusion Centre – Indian Ocean Region
IITs	Indian Institute of Science, Indian Institutes of Technology
IMO	International Maritime Organisation
IMT	International Mobile Telecommunication
IPCC	International Panel on Climate Change
ISR	Intelligence, surveillance and reconnaissance
ISRO	Indian Space Research Organisation
ITU	International Telecommunication Union
LAWS	Lethal Autonomous Weapons Systems
LBS	location-based services
MDA	Maritime Domain Awareness
MEA	Ministry of External Affairs
MERCOSUR	Mercado Común del Sur (Southern Common Market)
ML	Machine learning
MoU	Memorandum of Understanding
MQ	Multi-mission, uncrewed
mRNA	messenger ribonucleic acid
MTCR	Missile Technology Control Regime
NASA	National Aeronautics and Space Administration
NATO	North Atlantic Treaty Organisation
NITI	National Institution for Transforming India
NPT	Non-Proliferation Treaty
OECD	Organisation for Economic Cooperation and Development
PSA	Principal Scientific Adviser
QIA	Quantum Internet Alliance
QUIN	Quad Investors' Network
RAAF	Royal Australian Air Force
RAN	Radio Access Networks
RMIT	Royal Melbourne Institute of Technology
RNA	Ribonucleic acid
SA	Services and Systems Aspects
SATPI	Strategic and Technology Policy Initiative
SPS	Science for Peace and Security
SSN	submarine, nuclear powered
TA	Technology Assessment
TDIF	Trusted Digital Identity Framework
TGA	Therapeutic Goods Administration
TIA	Technology impact assessment
TSGs	Technical Specification Groups
UAV	Uncrewed Aerial Vehicles
UIDAI	Unique Identification Authority of India
UN	United Nations
UNCLOS	United Nations Convention on the Law of the Sea
UNCTAD	United Nations Conference on Trade and Development
UNSGM	United Nations Secretary General's Mechanism for Investigation of Chemical and Biological Weapons

WHO	World Health Organisation
WMD	Weapon of Mass Destruction

Introduction

This paper presents a case for India and Australia to adopt and champion consistent use of joint technology impact assessments (TIA) of critical technologies affecting peace and stability in their bilateral and multilateral diplomacy. It is the second research paper in a project on that topic funded by the Australia India Cyber and Critical Technologies Partnership (AICCTP). Our first paper (Austin et al. 2025) provides a comparative analysis of practices of both Australia and India for TIA in that field. It found that the two countries did not have an extensive or consistent approach to this activity, and that they "would benefit from a clearer commitment to regularised TIA" to support their diplomacy.

Austin et al. (2025) set benchmarks for how a country might undertake TIA with a focus on critical technologies for peace and stability. Without dictating a rigid framework, we proposed that stakeholders consider the following nine considerations as central:

- an appropriate balance in focus between a very broad class of technology and specific sub-fields where the impacts are discrete from other sub-fields (such as facial recognition tools within the broad class of AI technologies)
- depth and granularity of consultation with specialists
- breadth and depth of stakeholder consultation, especially community interests
- public transparency
- recognition of the principal place of the non-technical social, political, legal and economic impacts of technology use
- comprehensiveness of analysis, including international and alternative views
- timeliness
- high relevance to policy for peace and stability
- a clear ethical framework.

To qualify as a TIA for peace and stability, there has to be clear and concrete evidence of novel research already undertaken or underway. There have to be clear conclusions about the impact on broader political, social or economic aspects affecting peace and stability. We do not consider a dialogue, a proposal to undertake joint assessments, or scientific research limited to basic science to constitute a TIA. Informed speculation about the development trajectory of a class of technologies, such as AI or quantum, would not particularly useful TIA unless it is accompanied by considerable analysis of specific use cases of the technology.

Our first paper also identified three tiers of TIA by the degree to which a particular assessment process meets these benchmarks: (1) basic, (2) intermediate; and (3) advanced. Each level corresponds to how many of these criteria are addressed in a given TIA: "basic" applies to TIA where only a few of the nine criteria are addressed; "intermediate" applies where a reasonable number have been addressed; and "advanced" applies where all or almost all have been addressed. In this paper, we will apply this characterisation of levels.

TIA is an inherently political exercise, in which terms of reference for assessment are shaped explicitly or implicitly by preferred outcomes, and often to the advantage or disadvantage of specific actors.

This paper takes a holistic approach to TIA, locating it in a broader canvas of geopolitics, geo-economics, and history than was visible in our first paper. The distribution of technological power across the world, and the ambitions of many countries to destabilise (wholly or in part) this pre-existing balance of technological power, form the essential background to modern TIA for peace and stability. Perceived disruptions to the status quo are often met with hyperbolic narratives about the potential impacts; these can lead to extreme responses, often with undesired and unintended consequences.

This paper has four main sections: (1) existing cross-border approaches to TIA of critical technology affecting peace and stability; (2) existing diplomacy involving Australia and/or India, with aspects of joint assessment of critical technology affecting peace and stability; (3) the way forward for Australia and India to build joint TIA of critical technologies for peace and stability, including selected use cases for prospective joint TIA; and (4) a possible multilateral initiative led by Australia and India to strengthen TIA for peace and stability in the Indo-Pacific, especially through support of communities of practice. The conclusion brings together key points from the four sections.

1.1 Definitions

We limit our view of *peace and stability* to the diplomacy of international and national security. This includes political aspects of deterrence and issues of common or cooperative security among states, such as protection of global critical infrastructure, arms control, or plurilateral regimes for export controls such as the Wassenaar agreement (Austin et al. 2025a, pp. 1-2). The definition excludes Issues of national military security and defence preparedness, military aspects of alliance building, and defence diplomacy. We also exclude domestic security operations like counterterrorism or protection of civil rights, but we include international regimes for countering violent extremism or terrorist financing.

Policy for peace and stability, as we define it, therefore addresses issues such as peacekeeping, arms control, international cybersecurity, countering disinformation, conflict prevention, space situational awareness, counter-terrorism regimes, and the security of civil sector international interactions, such as air safety.

The scope and definition of "critical technologies affecting peace and stability" is less precise (Austin et al. 2025:2-5). In 2020, Australia and India agreed to a Joint Plan of Action specifically targeting, *inter alia*: (1) the innovation economy; (2) cyber security; and (3) cyber-enabled critical and emerging technologies (Austin et al. 2025:3). In the agreement, the last of these three topics was expressed in terms of the economy, making specific mention of 5G, quantum computing, and AI /machine learning (ML).

In relation to AI, the agreement mentioned the need to work bilaterally to build safe, trusted and ethical practices in its use. The Action Plan also referred to the importance of international norms for governing AI. The two governments have not been as transparent and consultative as they could be on the parameters by which they define and classify critical and emerging technologies, especially when it comes to differentiating between broad technology classes, such as quantum sensing, and more specific sub-fields, such as quantum radar or photonics.

We noted that the clear distinctions some see between TIA on the one hand and, on the other "technology assessment" (TA) without the emphasis on impact, is one that is frequently blurred in practice.

2. Cross-border Approaches

International TIA (or TA) for peace and stability are instruments used in diverse multilateral and bilateral settings, often against the backdrop of geopolitical turmoil and the emergence of disruptive technologies. As of 2025, there exists a plethora of effective multilateral and bilateral technology assessments and associated communities of practice. Through these activities, both Australia and India have demonstrated their commitment to joint technology impact assessments, even if a distinctly direct and bilateral aspect linking the two countries in these multilateral activities has been visible in only a small number of instances.

Sub-section 2.1 provides examples of multilateral collaboration in TIA, whether it is through peace and stability treaties, industry-related bodies like the Third Generation Partnership Project (3GPP) for wireless technologies, or state-based organisations such as UN agencies and regional organisations. Sub-section 2.2 addresses examples of bilateral TIA efforts where Australia and India have not been prominent. Sub-section 2.3 summarises the benefits and challenges of joint TIA fin general for peace and stability suggested by those examples.

2.1 Multilateral TIA

Longitudinal technology assessment on a multilateral basis is a normal element of diplomacy for peace and stability and has been for decades. Table 1 lists ten treaties from before 2000 that involved TA/TIA. In almost all of these treaty regimes, stakeholders from countries with diverse geopolitical positions on critical technology frequently exchange research to reconcile competing technology assessments affecting peace and stability. In some instances, joint investigations and research approximating TIA occur, even if at a basic level. On rare occasions, the information being exchanged has included data derived from sensitive intelligence sources.

Table 2 lists ten more recent treaties or Working Groups after 2000, where similar practices of formal or informal joint technology assessment take place, including reconciliation of competing assessments where the TIA practices applied were more consistently at the intermediate or advanced levels. These examples involve active scientific research, technology assessment, and often experimental programs—not just diplomatic or political dialogue.

Table 1: Ten Peace and Stability Treaties before 2000 with Continuous Technology Assessment

Treaty/Agreement	Technology Assessment Mechanism
Outer Space Treaty (OST) 1967	Prohibits the stationing of nuclear and other weapon of mass destruction (WMD) in space; establishes inspection, registration, and international consultation mechanisms for activities/technologies such as spacecraft, satellites, and lunar installations to avoid harmful interference and contamination
Treaty on the Non-Proliferation of Nuclear Weapons (NPT) 1968	Requires monitoring and safeguards for nuclear materials and technologies via the pr-existing International Atomic Energy Agency (IAEA); thorough inspection and audit of reactors, enrichment facilities, and nuclear fuel cycles to ensure non-diversion to weapons
Biological Weapons Convention (BWC) 1972	Prohibits biological weapons; periodic scientific and policy reviews assess biotechnology, diagnostic tools, and dual-use facilities with technical expert groups convened to track compliance
Convention on Certain Conventional Weapons (CCW) 1980	Restricts specific weapons (e.g., landmines, lasers); mandates periodic review conferences and technical working groups to assess new weapon systems and their humanitarian/technological impact
United Nations Convention on the Law of the Sea (UNCLOS) 1982	Regulates technologies like seabed mining, cable-laying, and shipping; requires environmental impact assessments and technology transfer for marine scientific research and resource extraction
SG Mechanism for Investigation of Chemical and Biological Weapons (UNSGM) 1987	Deploys accredited technical teams and labs to investigate alleged use of chemical/biological weapons using forensic sampling, detection, and analysis technology, guided by operational manuals and international standards
Missile Technology Control Regime (MTCR) 1987	Implements ongoing classification and control of technology related to missiles and UAVs capable of WMD delivery; assesses and regularly updates control lists via member state consultations
Chemical Weapons Convention (CWC) 1993	Enforces inspection and verification of chemical plants, weapons, and dual-use facilities; technical review and sampling of chemicals for verified destruction and compliance, with a sophisticated global monitoring and auditing system
Comprehensive Nuclear-Test-Ban Treaty (CTBT) 1996	Prohibits physical nuclear weapons testing; employs international monitoring systems (seismic, radionuclide, acoustic) and on-site inspection protocols to assess compliance using advanced detection technology
Wassenaar Arrangement (1996)	Multilateral export regime that assesses, and updates lists of conventional arms and dual-use technology; member states regularly hold technical meetings to review and define controlled technologies

Table 2: Ten Peace and Stability Treaties after 2000 with Continuous Technology Assessment

Treaty/Forum/Body	Technology Assessment Mechanism
Article 36 of Additional Protocol I to the Geneva Conventions (weapons review since 2000)	Requires states to legally review all new weapons, means, or methods of warfare, including emerging technologies, for compliance with international law and humanitarian obligations before development, procurement, or deployment
UN Group of Governmental Experts (GGE) on International Security Aspects of Information Technology (since 2002)	Conducts expert assessments of threats posed by ICTs, proposes international norms, and recommends best practices for states on technology use in the context of international security

UN GGE on Lethal Autonomous Weapons Systems (LAWS) (since 2016)	Examines compliance of autonomous weapons with international humanitarian law, guiding states to assess human-machine interaction, targeting, and risk mitigation in emerging weapon systems, and supports policy options and review protocols
OECD Recommendation on Artificial Intelligence (2019)	Provides principles and recommendations for trustworthy AI, with policy frameworks for assessing impacts, safety, accountability, and national/international metrics for AI systems
Global Partnership on Artificial Intelligence (GPAI) (launched 2020)	Supports collaborative research and policy benchmarking on AI safety, ethics, and societal impact, with expert working groups developing frameworks and technical tools for trustworthy AI assessment and deployment
World Economic Forum Global Technology Governance Summit and Councils (launched 2020)	Convenes stakeholders to discuss, benchmark, and recommend governance approaches for emerging technologies, emphasizing public-private collaboration, risk management, and standards for responsible deployment
US-EU Trade and Technology Council (TTC)(set up 2021)	Expert working groups meet to assess standards, risk management, regulatory alignment, supply chain security, and export controls on advanced technology, especially AI and semiconductor.
G7 Future Tech Forum and G7 AI Working Group (since 2021)	Coordinates G7-wide technology and AI policy assessment through shared research agendas, risk frameworks, and transparency guidelines, including reporting frameworks for advanced AI systems
OECD Global Forum on Technology (launched 2023)	Serves as a platform to share evidence, best practices, and coordinate international assessment of technology governance, standards, and regulatory responses among governments and stakeholders
Council of Europe Framework Convention on Artificial Intelligence, Human Rights, Democracy, and the Rule of Law (2024)	Establishes binding rules and standards for the assessment of AI technologies' impact on human rights and democracy, requiring member states to implement review and monitoring mechanisms for compliance and accountability

The operation of these international treaty regimes or arrangements depends on collaboration or contestation by the parties around the capabilities of various technologies and their impact on peace and stability. The following discussion further illustrates multilateral assessment for critical technologies affecting peace and stability, through international standard-setting arrangements, regional security organisations and international organisations.

The overwhelming share of multilateral TIA for peace and stability has been largely alliance-based, as in the Five Eyes or NATO, which had their origins during the Second World War. The emergence of the European Union as a unified political actor in foreign and economic policy after 1992 reinforced the existing record of TIA, and the future pre-eminence of those three groupings in TIA.

This alliance-based TIA activity coexisted at the multilateral level with what might be called functional agencies, such as the International Telecommunication Union (ITU) in existence since 1917, the International Civil Aviation Organisation (ICAO) since 1947, and the International Maritime Organisation (IMO) since 1948. Their joint TIA-based standard-setting in various civil sectors has, for the most part, contributed to international stability since the 1950s.

Multinational groupings outside NATO and the EU have undertaken joint TIAs for peace and stability at a much later date, with the BRICs (Brazil, Russia, India, China, and South Africa), for example, only moving in that direction between 2015 and 2025. Of special note for India and Australia, the Commonwealth (56 member states) has also been engaged in TIAs on a modest scale in the same time frame. Other regional organisations, such as the African Union (AU) and MERCOSUR in South America, have also been expanding their activities in this direction.

Australia and its researchers have been closely integrated in multilateral TIA for peace and stability undertaken within Western alliance arrangements and international organisations since the Second World War. The country has also been a consistent contributor to the work of the UN specialised agencies, and to TIA work with some regional bodies.

It has been an active and influential contributor to impact assessments of the International Panel on Climate Change (IPCC).

Since India has pursued a non-aligned diplomacy, Indian researchers did not contribute so visibly to alliance-related joint work on disruptive technologies after its independence, but it consistently engaged in shaping debates and the work of international organisations, most visibly the International Atomic Energy Agency (IAEA). India is not a signatory to the Non-Proliferation Treaty but is an influential founding member of the IAEA.

India has partnered both with nations from the Western bloc and their potential rivals on matters impacting peace and stability. For example, India has been collaborating with countries such as Russia and China through its participation in the BRICS since 2006, as well as with the Quad involving the US, Australia and Japan since 2020. Further, India has engaged with Russia on areas affecting peace and stability, such as cybersecurity, defence and AI. India also has a unique agreement with the US, which allows for civil nuclear cooperation.

2.1.1 FIVE EYES and AUKUS

Since the 1950s, the premier multilateral organisation for joint technology assessment affecting peace and stability has been the Five Eyes, a treaty-based arrangement involving Australia, Canada, New Zealand, the UK and the US. It has been this group which, in many respects, spawned a smaller trilateral arrangement (AUKUS) in 2021. The once dominant role of the Five Eyes in TIA has been increasingly complemented by the work of NATO, beginning as early as the 1960s, and that of the EU, beginning most conspicuously in the 1980s and 1990s.

It goes without saying that as an intelligence alliance, the work of the Five Eyes partners on TIA has not typically been characterised by public consultation or democratic accountability. There have been notable exceptions, mostly in the US and EU cases, where public oversight of the intelligence agencies has been more rigorous (as in the Echelon affair and the Snowden revelations).

Intelligence collection was the main purpose for the establishment of the Five Eyes, but the group has also operated intelligence in the parallel domain of intelligence assessment, including some forms of joint TIA. One might speculate that these countries collaborated on joint assessments of key technology milestones between 1950 and today, including:

- China's acquisition of nuclear weapons in 1964
- India's nuclear test in 1974
- Vietnam's alleged use of chemical weapons in Laos and Cambodia in the early 1980s
- Iraq's efforts to acquire WMD in the 1980s.

The Five Eyes have been more transparent and consultative in technology assessments in the past decade, especially in the case of cyber threats and responses. This can be seen very clearly in joint advisories released by Five Eyes agencies, which communicate important impacts of certain cyber tools or cyber actors (CISA 2021; CISA et al. 2024).

If we look just at the assessment side, the five intelligence allies, or sub-groups thereof, have undertaken joint TIA on various high-profile issues with significant global impact, not least alleged Iraqi weapons of mass destruction in 2002 and 2003 (Barnes 2020). Assessments by intelligence agencies are almost always non-transparent; nevertheless, especially in more recent years, many of these reflect community perceptions and interest in various ways, even if indirectly. Moreover, the public deliberations by US Congressional Committees and revelations by whistleblowers have revealed important details on the Five Eyes joint assessments (Boycott 2014). During the Cold War and after, the Five Eyes have consistently undertaken joint impact assessments of nuclear technologies, delivery vehicles, other advanced technologies, and foreign technological capabilities.

The AUKUS agreement, signed in 2021, has two pillars, one covering the transfer of nuclear-powered attack submarine (SSN) technology to Australia, and one covering intensified cooperation in joint assessments of advanced technology (Congressional Research Service 2024:13). The commitment to joint technology assessments under AUKUS (Australian Submarine Agency 2024:3; ARPANSA 2024:4-5) has its most prominent public-facing aspect in respect of management by all three parties of related nuclear waste, even though formally the agreement vests full responsibility for the management of that in Australia. Another illustration would be assessments of autonomous drones and AI/robotic systems measuring actual operational effectiveness, resilience, and interoperability (Australian Government Defence 2024).

2.1.2 NATO

NATO, its member states and its partner states have collectively amassed the greatest body of joint technology assessments of critical technologies affecting peace and stability. From the 1950s, NATO was interested in assessments of emerging and disruptive technologies, including nuclear propulsion (AGARD 1978). Within NATO, the first formal joint technology assessments were conducted by the Advisory Group for Aerospace Research and Development (AGARD) in 1952. This group rarely strayed from narrow technology performance assessments into broader social or economic impacts, so they represent only the basic level of TIA.

Similar activities were set up in other policy fields in that decade, including military and economic potential of member states. AGARD had several working groups, each having a representative from each country. At that time, the organisation of the civilian side of NATO was however addressing mainly one overarching question: "reassessment of the most effective pattern of military strength" (Lord Ismay 1954:108). The technical committees themselves were regarded as an instrument to bind the new alliance together, even if most of their joint TIAs did not specifically mention peace and stability issues.

In 1969, the US pushed NATO to take up the social and community impacts of technology through creation of a Committee on the Challenges of Modern Society (CCMS) (Turchetti 2010:8). The assessment work of that group continued until 2006 and is seen by some as leading directly to the 1972 UN Conference on the Human Environment in Stockholm and eventually the UN Panel on Climate Change (Turchetti 2010:8).

Around 2000, NATO interest in joint assessment of critical technologies affecting peace and stability became even stronger (Herzog and Kunertova 2024). A sizable share of the committee's studies by then were addressing subjects directly related to peace and stability, such as chemical munitions disposal, oil spill clean-up in conflict zones, dual-use technologies applicable to disaster relief and military engineering, post-conflict reconstruction, and NATO's civil emergency planning and environmental security strategies (NATO Archives n.d.).

In 2006, the CCMS merged with NATO's Science Committee to form the Science for Peace and Security (SPS) Program, with a brief to develop initiatives on security challenges, including environmental security, the prevention of natural catastrophes, and energy security. In 2021, NATO adopted an ambitious Climate Change and Security Action Plan to mainstream climate change considerations into NATO's political and military agenda. NATO's 2022 Strategic Concept sets the ambition for NATO to "become the leading international organisation when it comes to understanding and adapting to the impact of climate change on security" (NATO 2024). In 2023, SPS completed two multi-year projects in quantum sciences involving around 40 universities and research institutes (James 2023). A typical project has been the multi-year collaboration on secure quantum communications (Project G5985) beginning in 2023 and relying on joint technical assessment involving researchers and officials from four countries and directly related to peace and stability (NATO Project SPS G9895 n.d.).

2.1.3 European Union (EU)

The EU's Maastricht Treaty, signed in 1992, formalised the transformation of the European Community into a political union, with a unified foreign and security policy that had begun to emerge in the late 1980s. The Treaty specifically alludes to the objectives of "peace and security", as do its many revisions over 33 years.

The EU adopted a Common Foreign and Security Policy in 1993, and a separate Common Security and Defence Policy in 1999. The EU Treaty provides the mandate for both policies in Title V (Articles 21–46). Home affairs (law and justice) was nominally incorporated as an EU competency in the EU Treaty, but this was strengthened under the Amsterdam Treaty of 1999 establishing EU authorities for migration, asylum, and border controls, including counter-terrorism and cyber security.

The EU has developed elaborate systems for health technology impact assessment but has a less formalised approach to TIA for peace and stability (foreign affairs, defence and domestic security). The EU research funds, which are substantial, put significant emphasis on conducting joint TIA in support of peace and stability, mainly through Horizon Europe's Civil Security for Society cluster.

There is not always a formal, recurring requirement for joint TIAs for peace and stability, as exists for health TIA. Nevertheless, the growing incorporation of collaborative risk analysis, integration of scientific evidence into policymaking, and multinational project designs has positioned joint TIA as a central feature of EU policy in the security field.

One of the most interesting early TIA from the EU affecting peace and stability came in an extensive report of the European Parliament (EP) on its social impact analysis of US and allied intelligence operations and surveillance of EU citizens in preceding decades under the Echelon Program. According to the report, the investigations “galvanised European politicians and inflamed public opinion in a way achieved by few other parliamentary initiatives” (EPRS 2014:17), thus meeting the public engagement test which this paper sees as an essential criterion for TIA (Schmid 2001).

More recently in 2023, the European Commission (EC) committed to multilateral risk assessment of ten high-priority technologies, based on their potential to disrupt security, human rights, or the military balance, or to facilitate economic coercion (European Commission 2024:5, 9). This framework guides policy coordination across the EU, even as member states retain a number of national prerogatives, particularly in security. The ten technology areas addressed by the EU included: (1) Advanced Semiconductor Technologies; (2) AI; (3) quantum technologies; (4) biotechnologies; (5) advanced connectivity;, (6) navigation and digital technologies; (7) advanced sensing technologies; (8) space and propulsion technologies; (9) energy technologies; and (10) robotics and autonomous systems. The EU work is supported by a high-level expert group on the Economic and Societal Impact of Research and Innovation and the EU Observatory on Critical Technologies. These bodies do not appear to have published any unclassified technology assessments relating to peace and stability.

The EU Quantum Technologies Flagship initiative involves all EU Member States and some associated states with the aim of consolidating European leadership in quantum technologies. The primary objective is to establish a competitive quantum industry in the EU, inclusive of addressing peace and stability issues (European Commission and Quantum Flagship 2024:219).

The initiative explicitly addresses the dual-use potential of quantum technologies, the need for secure quantum communication infrastructure, and the importance of international governance to prevent destabilising uses of quantum systems. It points to the need for less geopolitical tension and new ways of handling technology innovation instead of a default recourse to military competition (European Commission and Quantum Flagship 2024:239). The effort involves direct participatory contributions from all 27 EU Member States and three associated countries (Switzerland, Norway and Israel in select projects).

The Flagship is coordinating EU-wide assessments of supply chain vulnerabilities and the dual-use (civil/military) potential of quantum technologies. These assessments focus on ensuring that quantum advances enhance European and international security, including the development of quantum-secure communications for critical infrastructure, space, and defence, and the management of technology risks that could destabilise global security if exploited by adversaries (European Commission 2025:1, 15). Projects funded by the Flagship are shown in Table 3. Most flagship projects involve large consortia of 5–20 countries, with some (like EuroQCI and QIA) involving nearly all EU Member States and some associated countries.

Table 3: EU Quantum Flagship Joint Assessments

Project	Sub-field	Countries	Peace and stability aspect
OpenSuperQ	Quantum computing infrastructure	DE, CH, SE, FI, NL, FR	Secure computing, strategic autonomy
QIA (Quantum Internet Alliance)	Quantum communication and networking	12+ countries including DE, NL, FR, IT, SE, DK, CH, UK	Secure communications, resilience
PASQuanS/PASQuanS2	Quantum simulation for complex systems	DE, FR, AT, IT, PL, ES	Modelling, security, scientific diplomacy
EuroQCI	Pan-European quantum communication infrastructure	All EU Member States, + NO, CH	Secure, resilient communications

2.1.4 OECD-UN Collaboration

OECD member states and the United Nations are collaborating on identifying priority benefits and risks of AI, emphasising the need for proactive policies to manage these risks and maximize benefits (OECD 2024a). The intent is to marry the global reach and influence of the UN to the unmatched analytical and technical capabilities of the OECD and its AI Observatory. The latter group already provides assessments that touch on peace and stability (OECD 2024b, 2024c, 2025a). This joint initiative is intended to develop additional assessments on AI risk and opportunity for the potential benefit of all UN members, as well as engage them directly in such assessments where practicable.

2.1.5 BRICS Quantum Computing Initiative

This initiative embraces collaboration not just on quantum science but on related uses of AI, cybersecurity and fintech. The work is underpinned by joint technology assessments, though these are pointed more to economic and technological goals than specific peace and stability ambitions. That said, BRICS and its technology efforts are intended to strengthen its members to enable them to better resist US and Western technological hegemony (Rachman 2025: 121).

The BRICS, initially bringing together just four countries, then five (Brazil, Russia, India, China, and South Africa), now has eleven members (Egypt, United Arab Emirates, Ethiopia, Indonesia, Iran, Saudi Arabia). Some of the newer members are not yet part of the Quantum initiative.

The evolution of BRICS technology collaboration, which began in 2006, has gathered pace since 2020 (Die 2025). In the quantum field, there have been substantial achievements, based in part on joint assessments. These have been largely based on bilateral efforts among BRICS founder members, especially Russia and China, even though India may be ahead of Russia in quantum research and applications. The main milestones have been a China–Russia Quantum Communication Link between Wulumuqi in western China and a station outside Moscow (Swayne 2024).

2.1.6 Wireless Technologies: Case Study for UN Specialised Agencies

The impact of wireless technologies of the 5th and 6th generations (5G and 6G) on peace and stability will be profound. This has been spelt out in a study by the International Institute for Strategic Studies (IISS) on 6G competition between the United States and China (Lee et al. 2022). The joint TIA that have emerged through this process are some of the best examples of such activities, which also occur regularly in the work of other UN specialised agencies, like the International Maritime Organisation (IMO), the International Civil Aviation Organisation (ICAO), and the World Health Organisation (UNCTAD 2022; ICAO 2018; WHO 2025).

While at one level issues of wireless technology may appear to be an exclusively domestic civil sector activity, the experience of recent years is that most states and key industry players regard the technology as one of the most significant technologies affecting peace and stability. 6G technology is being developed for military applications, such as enhancing electronic warfare and missile guidance. It also includes systems designed to mislead enemy radar and create decoy targets. Additionally, 6G aims to provide high-speed, reliable data links for missile control, particularly for hypersonic vehicles and to address communication disruptions caused by plasma sheaths.

There are also divergences in the visions for the future of 6G between states. For instance, China's IMT 2020 6G Promotion Group is pushing for high-precision positioning information that could further political control over society and the economy (Rühlig 2021: 69). On the other hand, 6G is regarded as having the potential to better service rural and remote areas in developing countries and to significantly enhance commercial and social opportunities in ways that promote political stability and domestic security.

The 3rd Generation Partnership Project (3GPP) is a global consortium that brings together the seven leading regional standards organisations and hundreds of industry stakeholders, including government representatives, to develop technical specifications for mobile telecommunications, including 5G and 6G technologies (Schmitt 2024). Its standards-setting process is deeply collaborative and multilateral, ensuring that new technologies are rigorously assessed and harmonized for global interoperability. 3GPP is organised around three main Technical Specification Groups (TSGs) – Radio Access Networks (RAN), Services and Systems Aspects (SA), and Core Network and Terminals (CT).

3GPP operates in tandem with standard setting by the UN's specialised agency, the ITU (Henry et al. 2020). The joint technology assessment processes are rigorous and transparent. Assessments can pass through several stages, all of them exposed to comment by a very large community. The central elements are Study Items, Work Items, Technical Reports and Change Requests.

The 3GPP also submits its analysis to independent external evaluation. 3GPP can host up to 20 plenary meetings in one year, each meeting typically attracting 600–2,000 participants, with more specialised working group meetings drawing several hundred delegates. Over a given year, the total number of unique stakeholders actively participating in meetings and submitting reports is around 700–800 organisations, with thousands of individual experts involved.

While geopolitical tensions swirl around the deployment and potential misuses of wireless technology for espionage, 3GPP and its work remains a compelling example of the value and potential of open and consultative multilateral technology assessment for peace and stability (Bruer and Brake 2021; Bojić et al. 2021; Chow and Ma 2022; Lipford et al 2025).

Chinese state support for its telecommunications companies and push for greater presence in standard setting and patents has led to concerns about undue influence of Chinese companies in the operations of the 3GPP (Rühlig 2021). This has also led to the US and other countries (including Australia and India) pushing for Open RAN, which disaggregates the network and allows interoperability between telecommunication vendors, thereby reducing barriers to market entry (Reddy 2023). However, the Open RAN technology comes with its own problems, related to increased threat surface for cybersecurity attacks and challenges in integrating complex equipment from different vendors.

The United States, the United Kingdom, Australia, and India have restricted Chinese companies such as Huawei and ZTE from participating in core telecommunications infrastructure projects. This decision stems from concerns about potential Chinese government influence, espionage claims, security of supply chains, intellectual property theft and broader geopolitical tensions. Despite there being competing interpretations of such allegations, national security considerations have outweighed other market considerations for those governments in imposing restrictions on Chinese companies (Lacey 2020).

Despite these concerns, wider active participation in the standards organisations represents the best way forward for promoting trust. 3GPP's SA3 working group is responsible for defining requirements, specifying architectures, and developing protocols for security and privacy in 3GPP mobile systems, including 4G, 5G, and beyond. The group's outputs are foundational for the security of global mobile networks and are widely cited in both academic and technical literature (3GPP 2024).

There are several academic analyses of the effectiveness of the work of SA3, with one being particularly informative about the indicative value and shortcomings of the effort on standards for surveillance technologies (Becker et al. 2024). It finds that European and US governments actively shape surveillance standards in 3GPP, but the Chinese government is less involved directly, leading to distrust about the role of Chinese companies. It argues that deeper integration of the Chinese government in this work in 3GPP could serve as a "trust-building measure for international peace and stability". Several states, however, retain serious concerns about the links between Chinese corporations, especially Huawei, and China's intelligence and security agencies.

2.2 Bilateral TIA for Peace and Stability

Compared with multilateral TIA, exclusively bilateral joint TIA appear to be less visible in the public domain; however, they have been an ongoing effort in international relations since the US and UK cooperated in dual-use technology policy before and during World War II (Macleod 1994; Connor 2015). Here we offer several examples of other bilateral TIA, even if these are not always presented as such.

2.2.1 Russia/US on Iran Nuclear and Missile Threat

In 2007, a high-level US/Russia Track 1.5 meeting in Moscow agreed to attempt to resolve a sharp disagreement between the two countries about the impact on European peace and stability of development by Iran of its nuclear and missile potential (EastWest Institute 2009).

As a track 1.5 affair, the meeting included some very high-profile people, including former CIA, former KGB, and serving Russian intelligence advisers, including the Special Representative of the President for Counter-Terrorism. On the US side, there was retired General James L. Jones, who subsequently became the US Secretary of State, and retired General Lance Lord, a former commander of US Air Force Space Command.

After around one year of joint meetings and investigation of technological parameters of Iranian capability, the two countries did not agree on the Iranian nuclear and missile threat to Europe. The disagreement focused on the US deployment to Eastern Europe of anti-ballistic-missile radar, ostensibly for early warning of an Iranian missile attack. Russia discounted this premise, believing instead that the radar was intended to track their missiles.

To address this disagreement, Russia and the United States agreed to set up a joint task force of technical specialists from both sides to try to reach a consensus on an assessment of the ballistic missile and nuclear capabilities of Iran. It was, in essence, a cooperative activity between some of the best specialists in the United States and in Russia. Each team had government connections, though these were more direct on the Russian side. The EastWest Institute published the joint assessment in 2009 after about a year and a half of work. The report was front-page news in several Western newspapers, especially in the US, when it was published.

This was a strong example of how two countries, even in the midst of a tense disagreement and as relations were slowly deteriorating, can actually come together to do a joint technology assessment, calling upon their best experts. Findings of the joint assessment were formally briefed to the US National Security Advisor, the Russian Foreign Minister and the Secretary of the Russian Security Council (EastWest Institute 2009:ii). On missiles, the report concluded that "there is at present no IRBM/ICBM threat [to Europe] from Iran and that such a threat, even if it were to emerge, is not imminent" (EastWest Institute 2009:17). On nuclear threats, the task force agreed that the "more immediate danger comes from the military and political consequences that would follow if Iran were to acquire nuclear weapons" (EastWest Institute 2009:17).

2.2.2 US Bilateral Initiatives

We can point to many examples of bilateral TIA for peace and stability, ranging from basic to advanced levels, mainly among the more developed economies. Many of those involving the US stand out for their systematic, co-authored, and data-driven approach to assessment, involving novel research on both the technologies and their impact.

Bilateral US-Canada research led to field trials of AI-based situational awareness assistants (e.g., NASA's AUDREY system) with Canadian paramedics, measuring effects on decision-making and impacts, supported by peer-reviewed publications (DHS 2020). We can note that Canada's AI algorithmic assessment initiative is an excellent example of TIA (World Privacy Forum 2024).

The joint University of Tokyo–IBM Quantum Hardware Test Center was launched in 2021 as the world's first dedicated site for the testing and evaluation of quantum hardware components (IBM Quantum 2025). This initiative is core to the broader US–Japan Quantum Innovation Initiative Consortium and regularly brings together IBM and major Japanese component makers (TDK, Kyocera, Fujikura, I-PEX, ULVAC) to perform systematic testing, benchmarking, and resilience assessments of components. Testing includes *cryogenic microwave isolators, superconducting wiring, dilution refrigerators*, and large-scale quantum chip packaging. Empirical performance results inform both ecosystem resilience analysis and practical supply chain adjustments, as new component capabilities and reliability data directly shape procurement and engineering strategies in both countries.

2.2.3 US-China and Joint AI Safety Research

There is a bilateral US/China project that is relevant even if it is undertaken without heavy involvement of officials of the two countries and their stakeholders. It is not a TIA, but it highlights the importance of TIA in this critical technology, especially where China and the US are involved (Imbrie and Kania 2024: 18). This is the project under the Center for Security and Emerging Technology (CSET) at Georgetown and the Center for International Strategic Studies (CISS) at Tsinghua University, fostering transparency in AI safety research despite geopolitical tensions (Siddiqui et al. 2025; CISS 2024). The project includes literature reviews and collaborative risk assessments (Siddiqui et al 2025, Zhang and Allen 2025).

There is a large unmet demand for bilateral and multilateral impact assessment of all aspects of AI, especially the safety of algorithms. Generative AI models have pushed the boundaries of what was imagined as the frontier of artificial intelligence in a very short period of time. In the past few years, the capabilities of generative models have scaled exponentially, with the compute being used for training during the development phase and inference post-deployment based on queries (Sevilla et al 2022). Generative AI models are general-purpose technologies with several use cases across many sectors, from academic research to healthcare to customer support to creative work. The regulatory gap between technology adoption and regulation, typically seen with emerging technologies, seems even more stark considering the pace of innovation and the scale of impact.

The imperfect nature of such models such as their tendency to hallucinate and generate factually incorrect outputs and the fast pace of adoption across various applications raises several concerns. These include protecting users from harms, mitigating the impact on the economy, environment, and social welfare.

Narratives about a given technology help shape public opinion, influence policy, and mobilise resources. The narratives of a US-China tech war have been gaining prominence, shrinking the space for cooperation (Retzmann 2025) and leading to national security emerging as the top priority in governing emerging technologies.

For example, the recently released America's AI Action Plan (The White House 2025) recognises AI as an area in which the US needs to "maintain unquestioned and unchallenged global technological dominance". This framing pushes the many serious governance concerns about AI, such as building guardrails or mitigating societal impact, to a lower priority.

Among AI experts, opinions about the future path of the technology are quite divided. Some experts postulate that we could see artificial general intelligence or AGI (AI capable of performing any intellectual task a human can do, across diverse domains without needing retraining) is just a few years away. Others feel that current approaches are unlikely to succeed and many other technological breakthroughs might be required before reaching AGI (AI Now Institute 2025). The former scenario lends itself to a race narrative that confers massive economic and military advantages to states that are at the frontier of the technology, while the latter scenario still positions AI as a very capable general-purpose technology that can have transformational impacts across all sectors.

The tech war narrative promotes a race to have a pro-innovation regulatory environment, so that domestic companies do not fall behind. A concerted global effort with active participation from the US and China is necessary to understand and mitigate the risks from AI adoption, by establishing intergovernmental dialogues on national security-related risks and building guardrails to ensure reliability and accountability.

In spite of international security sensitivities, there is substantial potential for detailed multinational assessments of AI algorithms, thanks to advances in collaborative frameworks and privacy-preserving technologies. International groups – such as the International Network of AI Safety Institutes and the OECD AI Observatory – enable countries to jointly develop testing standards and evaluation methods without fully sharing sensitive data or code.

2.3 Benefits and Challenges of Joint TIA

Joint TIAs are recognised as tools for fostering international cooperation, enhancing security governance, and promoting responsible innovation. Whether aimed at addressing emerging technologies like 6G and AI, or mitigating risks around dual-use military systems, TIAs offer structured opportunities for shared learning, conflict resolution, and forward-looking policymaking. At the same time, there is considerable room for states to make far more use of joint TIAs, and to make them more purposeful and actionable in the global quest for peace and stability.

Such activities can provide positive outcomes for problem-solving in the field of peace and stability, such as trust-building across adversarial or uneasy relationships, enabling multi-stakeholder visibility, promoting standardisation, and harnessing shared priorities. Mixed results from current and past joint TIAs underscore several tensions. Multilateral groups may struggle with divergent timelines, priorities, and norms. Government-led TIAs without civil society input risk being narrow or exclusionary. Technical depth may not always translate into policy adoption or democratic legitimacy.

There are other challenges for joint TIAs. Through roundtable discussions and formal commentary, the participants outlined recurring challenges. These included:

Strategic Asymmetry: When countries possess unequal technological maturity or diverging defence postures, joint TIAs can become contentious. Military technologies like autonomous weapon systems may be less tractable to policy consensus, and impact assessments of their use often face resistance to transparency or external validation due to national interest concerns.

Geopolitical Ambiguity: Further, where countries have divergent geopolitical, diplomatic, economic or foreign policy goals, they are less likely to cooperate on a joint TIA, even where the technology or supporting industrial infrastructure would clearly benefit. For example, the US and China will likely never conduct a joint TIA on certain technologies with high military or economic value (like semiconductors).

A Crisis of Authority: The formal structure and processes of politics and governance are a product of the Industrial Age. The emergence of powerful ICT utilities (such as Microsoft, Google and Meta) with a global reach and more power than most individual countries have produced a crisis of authority. Deliberative and democratic decision-making is increasingly challenged due to the fast pace of globally distributed technology innovation, the shrinking of attention span among legislators and regulators, the spread of disinformation, the polarisation of political discourse and the limited durability of policy narratives.

Institutional Gaps and Ownership: Many countries lack a centralised department for technology impact governance. Without clearly mandated bodies, TIAs often fall between ministerial silos, limiting strategic uptake and continuity.

Standardisation and Access: Closed-door standards development, especially in telecom and data security, limits the participation of smaller or less wealthy countries. Australian and Indian experts emphasise the need for open standards akin to OpenID, where broader communities can contribute to protocol evolution.

Data Sovereignty and Regulatory Fragmentation: Trust registries, identity authentication systems, and cross-border financial exchanges all suffer from mismatched data privacy laws and limited interoperability. Differences in the definition and implementation of cybersecurity measures further complicate joint assessments in these sectors.

Timing and Purpose: Whether TIAs are undertaken before deployment, during use, or after rollout determines their relevance and impact. A shared methodology and clarity on purpose are often missing, making TIAs inconsistent in methodology, style and credibility.

Lack of Gender and Inclusivity Focus: Technology impact assessments rarely integrate perspectives from women, marginalised communities, or private citizens affected by emergent disruptions. Anecdotal evidence (e.g., irrigation redesign by the Food and Agriculture Organisation involving women farmers) demonstrates that gender-aware assessment improves outcomes, yet this remains the exception rather than the norm.

2.3.1 International Structures

Bodies like the Intergovernmental Panel on Climate Change (IPCC) (climate), IAEA (nuclear), and ITU (telecom) do provide benchmarks in joint TIA. However, they are often slow-moving and domain-specific; not agile enough for technologies like AI or quantum computing.

Regional institutions and networks, such as ASEAN, the EU, and the Quad, offer diplomatic scaffolding, but their operational assessment capacity is limited. The EU is one of the better-positioned organisations because of its wealth and global position in science and technology. Tiered regional frameworks can be created based on the likely footprint of impacts of particular technologies.

Academic partnerships are essential components of all TIAs, but there is a risk of “projectisation” or fragmentation of strategic focus, where the partner scholars usually must apply on an ad hoc basis for small-scale grants rather than serve in standing well-funded research organisations dedicated to peace and stability. There may also be commercial or intellectual property aspects to TIAs that sit uneasily with the “open science” mindset common to many Western academic institutions.

Think tanks and civil society organisations that participate in joint TIAs are more common and stronger in the US and Europe (e.g., The Stimson Center and Electronic Frontier Foundation in the US) but underdeveloped or under-funded in most countries, including Australia and India. There is potential in forming cross-border coalitions that blend academia, policy advocacy, and private sector feedback in order to overcome the limitations of individual institutions. The non-government organisations best placed in Australia and India for joint TIAs will be the academies of sciences or peak bodies, such as Australian Information Security Association (AISA) and the Data Security Council of India (DSCI) for advanced information technologies.

3. Existing Australia-India Collaborative Activities

The foundations for future growth in Australia India Joint TIAs supporting peace and stability may be better than for any other Australian partner country outside the Five Eyes. This situation arises because of high untapped potential (starting from a low base), substantial bilateral scientific research activities over two decades, a shared official language, and the closer harmonisation of Australian and Indian strategic policy since 2020. Collaborations between Australia and India are growing rapidly. Moreover, there has been an expansion in trilateral scientific ties between Australia, India, and Japan since 2015, and quadrilateral ties, inclusive also of the US since 2017 (Chacko and Wilson 2020). These have been premised on growing commonalities of strategic interest among these countries.

The current state of play between Australia and India is captured by the agreement, announced by Australia on 3 July 2025, for the "first" defence science and technology project arrangement for mutual security with India (Australian Government. Defence 2025a). The project will provide a joint assessment of technologies relating to joint maritime sub-surface surveillance and situational awareness, a foundation stone for regional peace and stability.

The project will run over three years under the auspices of the Information Services Division of Australia's DSTG and the Naval Physical and Oceanographic Laboratory of India's Defence Research and Development Organisation (DRDO). They will jointly investigate the impact on surveillance goals of Towed Array Target Motion Analysis. This is a "collective term for target tracking algorithms, developed to estimate the state of a moving target". It is the "crucial element in maintaining platform situational awareness, when a passive mode of operation is required" (Australian Government. Defence 2025a). A towed array consists of a long linear array of hydrophones, towed behind a submarine or surface ship on a flexible cable. The joint project will put novel algorithms to the test, using the strengths and shared knowledge of the two countries. The project arrangement will include the "sharing of ideas, investigation trials, algorithm demonstrations and performance analysis". The two countries are prioritising improvements in surveillance capabilities in part to respond to the increased use of autonomous vehicles.

Australia does not have an AI safety institute, but India does. Techniques like federated learning and secure computation can allow stakeholders to validate model behaviour collectively while protecting proprietary information. Much of contemporary AI safety assessment— such as studies on alignment, robustness, bias, and broad societal impacts — can be conducted collaboratively within an academic/industrial framework, before models are weaponised or tightly controlled for proprietary or national security reasons. Joint "red teaming" and evaluation exercises can occur in secure environments, allowing countries to probe AI safety while maintaining necessary controls over sensitive assets.

It is worth noting that transnational collaborations on emerging, critical or disruptive technologies – especially with countries that Australia and/or India consider autocratic or lacking in institutional autonomy – will likely trigger exposure to export controls, sanctions and other national security implications. Aspects of research security, such as the protection of university research and development from national security threat actors, are beyond the scope of this paper; however, such issues may well require elucidation in any TIA policies enacted by both countries. In such cases, projects could be limited only to external scrutiny, like in black-box testing, with broader participation banned. Neutral international organisations can help by coordinating independent assessments and bridging trust divides.

3.1 Australia-India Strategic Research Fund

The Australia India Strategic Research Fund (AISRF), set up in 2006, has supported over 370 collaborative scientific activities (Australian Government. DISR 2025). There are 20 shared priorities, including quantum computing and communications, biotechnology for improved agricultural productivity and climate resilience, and RNA vaccines (Australian Government. DISR n.d.). Very few of these activities have been directly related to peace, stability, or security. Recent rounds have prioritised critical technologies such as quantum computing and communications, as well as biotechnology. The purpose of the AISRF was strategic: to foster joint research in the interests of mutual prosperity and security.

3.2 Australia India Cyber and Critical Technologies Partnership

Bilateral projects with a stronger security angle emerged in Round 4 of the AICCTP where a direct link with peace and stability appeared for the first time in its grant guidelines. A list of the projects approved in Rounds 1-4 can be seen in Table 4. While individual projects might not have carried an explicit reference to peace and stability, the overall purpose of the AICCTP program was to foster those geopolitical ambitions. The number of personnel and activities involved in AICCTP projects provided a substantial complement to work on critical technologies undertaken under the AISRF, though AICCTP projects had a stronger public policy focus.

Table 4: Focus of Projects funded by AICCTP 2021-24

Round 4 (announced 2024)
Securing the Internet's Backbone: Developing an Australia-India Framework for Strengthening Submarine Cable Connectivity, Resilience and Supply Chains
Joint Impact Assessment of Critical Emerging Technologies in Support of Peace and Stability
Foundational Principles for Responsible Development and Use of Quantum Technologies in the Indo-Pacific Region
A Paradigmatic Shift in Public Service Delivery: Accessible, Inclusive, and Secure DPI
Developing an Ethical Framework for using Blockchain-based Digital Credential Systems: Tackling the issue of Fake Degrees
Inclusive Digital Public Infrastructure (DPIs) to advance innovation in the Indo-Pacific
Round 3 (announced 2023)
Standardisation and Development of Practical Privacy-Enhancing Cryptographic Techniques for Cloud Computing
Critical Quantum Technology: Creating Scientific Fluency, Ethical Awareness and Policy Options for a Quantum Future
Effective Ethical Frameworks for the State as an Enabler of Innovation
Responsible Al for Net Zero – An Australian and Indian Collaborative Approach
New Ethical Frameworks for Synthetic Biology in the Indo-Pacific
101:BUILD: Building Inclusivity by Design in AI/ML Powered Healthtech: an Indo-Australian Partnership for International Policy Making
Round 2 (announced 2022)
Shaping blockchain technical standards consistent with Australia and India's shared vision of an open, free, rules-based Indo-Pacific
Cross Border Data Flows Between Australia and India: Understanding the legal, policy, and ethical standards for data, cyber security, AI, quantum, and new technologies
A techdiplomacy and negotiation guide on technical standards for Artificial Intelligence in the Indo-Pacific
Ethical 6G – Identifying Elements of Ethical Framework for 6G and Creating Opportunities for India and Australia
Round 1 (announced 2021)
Next Generation Telecommunications Networks: Privacy and Security Challenges, Regulatory Interventions and Policy Framework Project
Quantum Meta-ethics: A Project to Develop Normative Frameworks, Best Practices and Effective Accords for Emerging Quantum Technologies
Operationalising Ethical Frameworks in the critical technologies industries operating in India and Australia

3.3 Quad Quantum Centre of Excellence

In July 2024, the Quantum Centre of Excellence, set up by the Quad Investors Network a year earlier, published a joint assessment on 'Quantum Science & Technology in the QUAD Nations: Landscape and Opportunities' (QUIN 2024). The report draws on coordinated work by expert task forces across the four countries.

The 2024 report appears to be based on four task force reports: the quantum workforce and ecosystem, quantum computing, quantum communication, and quantum sensing. It surveyed the quantum landscape in each country, benchmarking strengths and identifying capability gaps. It also discussed shared challenges across domains like R&D infrastructure, human capital, regulatory hurdles, supply chain vulnerabilities, and market readiness. It proposed collaborative testbeds, technology sharing, and workforce strategies.

QUIN is a "network of investors, industry, and innovators" from the four countries (QUIN 2024, p. 56). The report discussed potential impacts only in very broad terms. The policy focus of the task force reports appears to have been economic and technological potential rather than a detailed analysis of the social or economic impacts of deployed technologies or on their impact on peace and stability.

4.Toward Joint TIA

Our earlier paper has highlighted the emergence of TIA as a necessary tool for anticipating and managing the peace and stability implications of critical emerging technologies. However, due to the novel nature of these technologies, most countries will only have access to a limited pool of experts to undertake such TIA. The complexity and pace of technological change strain the analytical capabilities of individual countries, necessitating collaborative approaches to understanding and managing their implications.

Modern TIA requires integration of multiple analytical domains: assessment of technical feasibility, analysis of strategic implications, ethical evaluation, regulatory impact assessment and studying societal acceptance or impact. The multidisciplinary nature of this work demands expertise spanning engineering, computer science, economics, military strategy, international relations, diplomacy, ethics, law and social sciences. This underscores the importance of international cooperation in TIA, particularly among nations with aligned interests and complementary capabilities.

The partnership between Australia and India has deepened over the last decade or so. A relationship that started based on "Commonwealth, cricket, and curry" (Layton 2023) has now transformed into a comprehensive strategic partnership. The reciprocal visits by the Prime Ministers of Australia and India in 2014 were historic. The Indian Prime Minister's visit was not just the first such visit by an Indian Prime Minister for nearly three decades but also included an address to a joint sitting of both houses of the Parliament – the first time an Indian Prime Minister had done so.

In 2017, the partnership was further strengthened through participation in the Quadrilateral Security Dialogue (Quad) alongside the United States and Japan, representing a diplomatic partnership committed to supporting a peaceful, stable and prosperous global order.

The bilateral partnership reached a watershed moment in June 2020, when Australia and India upgraded their relationship to the level of a Comprehensive Strategic Partnership (CSP). Both countries are committed to a free, open, stable, inclusive and rules-based Indo-Pacific, a vision that is increasingly being challenged by strategic competition and the erosion of established norms.

While there have been some hiccups in the relationship between 2020 and 2024 (due to allegations of espionage activities conducted by Indian operatives in Australia), the two countries appear to have put those ructions in the relationship behind them by 2025. This year, several major exchanges have occurred, including the first official visit to Australia by India's Chief of Defence Staff, the 9th Australia-India Defence Policy Talks (DPTs), visit to India as part of South and Southeast Asia trip to mark the 5th anniversary of the CSP by Australia's Deputy Prime Minister (also serving as Defence Minister), and a high-level Australia-India-Indonesia maritime security dialogue in Canberra (Australian Government. Defence 2025b, 2025c, 2025d).

The strengthening bilateral relationship between Australia and India and their mutual concerns regarding technological sovereignty, supply chain resilience, foreign interference and technology-enabled authoritarianism provide a conducive opportunity for collaborative TIA, especially in technological domains where both countries face common challenges and share strategic interests.

Australia and India share fundamental interests in maintaining freedom of navigation and secure maritime domains in the Indo-Pacific, which could be impacted by the advancements in maritime technologies, including autonomous underwater vehicles, advanced radar systems and satellite-based surveillance capabilities. Both Australia and India have experienced significant cyber threats from state and non-state actors, especially concerning critical infrastructure. The convergence of emerging technologies, including quantum computing, artificial intelligence, and 5G networks, creates new cybersecurity challenges that require sophisticated analytical capabilities.

The increasing militarisation of space presents common challenges for both nations. The development of space-based solar power, advanced satellite constellations and space-based manufacturing capabilities raises questions of mutual interest for the two countries about the future of space governance and the potential for space-based conflicts.

4.1 Synergies for Joint TIA

Both Australia and India possess complementary technological capabilities and shared democratic values that together offer a powerful synergy for a joint TIA programme. Australia brings world-class R&D in niche technologies like quantum, abundant critical minerals and a mature regulatory environment. India contributes a vast digital economy, global IT and software expertise, a dynamic startup ecosystem and a frugal innovation mindset. Together, they combine Australia’s deep-tech and regulatory rigour with India’s scale, agility and implementation capability – creating an ideal blend of scientific depth and real-world impact for effective TIA.

Both countries are developing advanced maritime technologies, including autonomous underwater vehicles, advanced radar systems and satellite-based surveillance capabilities. Australia's advanced biotechnology sector and India's large pharmaceutical industry create complementary capabilities for biotechnology TIA.

Australia's participation in the Five Eyes intelligence alliance and India's growing space capabilities create shared interests in understanding how emerging space technologies might affect regional stability. India's space program, led by the Indian Space Research Organisation (ISRO), has also demonstrated remarkable cost-effectiveness in developing advanced space technologies. Australia is still in the early stages of operating in space.

The Australian university system's strong connections to international research networks provide access to cutting-edge research. The Indian Institute of Science, Indian Institutes of Technology (IITs) and other premier research institutions in India have developed strong capabilities in emerging areas such as artificial intelligence and biotechnology. India also provides a large pool of skilled engineers.

4.2 Principles for Collaboration

It is inevitable that the two countries will have diverging national perspectives on the objectives and methodologies of TIA in certain scenarios. To be effective and sustainable, the joint TIA initiative should be guided by a set of core principles. Each candidate project for the conduct of joint TIA should be assessed against these principles to aid the two countries in defining and agreeing upon appropriate tasking statements. The following six normative and functional principles could be considered to act as a guide for the two countries.

Mutual benefit and reciprocity: Collaboration for joint TIA must provide both the countries valuable insights and opportunity to build capabilities, regardless of any imbalance in contributions of expertise and resources.

Shared values: Both Australia and India are committed to responsible technology development and deployment that respects human rights, rule of law, and social welfare, while enhancing rather than undermining international stability. This principle necessitates developing shared ethical frameworks for technology assessment, establishing mechanisms for public consultation and stakeholder engagement, and ensuring that collaborative outputs contribute to responsible technology governance rather than purely competitive advantage.

Respect for sovereignty: While promoting collaboration, the framework must respect the national sovereignty and independent decision-making of not just the two countries but also all other impacted countries. The findings of joint assessments should be considered as inputs to national policy processes, not necessarily as binding directives to dictate domestic policy.

Transparency and trust: Transparent information-sharing protocols must be developed, to provide assurance to each party that their partners are sharing accurate information and not withholding critical insights. Trust can be built by beginning with less sensitive topics and progressively expanding to more critical areas as confidence develops.

Institutional support: The partnership must focus on initiatives that can continue despite changes in government leadership. This means embedding collaboration in institutional frameworks, rather than relying solely on individual relationships or transient political alignments.

Evidence-based decision making: This can be achieved through a combination of qualitative and quantitative assessments based on scenario modelling, stakeholder interviews and field trials, as would be appropriate based on the maturity of the technology under assessment.

Clear code of conduct: Establishing a clear and concise code of conduct will enable maintenance of professional standards and ethical integrity throughout the collaboration. The code of conduct should also provide mechanisms for reporting ethical concerns and establish guidelines for data sharing.

4.3 Tiered model

To be successful, bilateral TIA needs to develop effective multistakeholder governance models. One focus of such a model should be transdisciplinary panels, longitudinal studies, and risk registers, which are key ingredients for sustained assessment capacity.

A valuable adjunct measure would be the development of a joint training framework for practitioners. A professional development curriculum tailored to Australia and India could seed common analytical frameworks. Topics could include standards assessment, diplomatic considerations, dual-use technologies, and stakeholder engagement.

These would ideally be shaped in support of building communities of practice, with different models reflecting unique sectoral characteristics. We could imagine distinct communities of practice (as we see already) for groups focused on cybersecurity, telecom standards, AI ethics, or critical minerals. The aim must be to foster depth and continuity. These could include academic clusters, think tank forums, or cross-country task forces with diplomatic support.

4.4 Building Communities of Practice

To maximise gains from new cooperation on TIA, Australia and India will need to consider how to boost national Communities of Practice (CoPs) for TIA. A CoP is a group of people who share a concern or a passion for something they do and learn how to do it better as they interact regularly (Wenger-Trayner and Wenger-Trayner 2015). These communities should involve a wide range of stakeholders from government, academia, industry and civil society in both countries. This will ensure a diversity of perspectives and a more holistic assessment of technological impacts. The CoP model will also provide agility to the TIA exercise, which then enhances the effectiveness of the assessment.

The CoPs can then be leveraged to identify emerging technology domains that would be a good candidate for joint TIA between Australia and India. This will enable a two-tier model consisting of the CoPs in each country, which could then be federated for collaboration across the two countries, facilitated by the specified nodal agency in each country.

The communities of practice may be more successful if they are focused on sub-regions or city clusters in participating countries. Given federal political constraints in countries like Australia and India, subnational governments at the state level (e.g., Victoria in Australia or Karnataka in India) could spearhead cooperation in building communities of practice in TIA.

We would ideally see clear inclusion of gender and rights-led frameworks at the outset. Stakeholder diversity (inclusive of the third sector and civil society), gender analysis, consideration of marginalised groups, and diversity of disciplinary backgrounds, improves quality and public legitimacy. Rights-based indicators can inform design and enforcement protocols.

There needs to be considerable diversity in assessment models. Ideally, TIAs should be longitudinal, revisited periodically, and linked to regulatory updates and public consultation mechanisms. Impact registries and sandbox environments may help test implications before roll-out.

Countries keen to extend joint TIAs can link them more directly to the advancement of open standardisation, data transparency, and security protocols. They should also provide dedicated public policy mandates and funding, alongside supportive institutional reforms to provide more explicit formalisation of pathways for joint TIA. Diplomatic engagement must reinforce collaborative ethics and conflict-prevention incentives.

By 2025, Australia and India have accumulated considerable good will and substantial experience of collaboration in science and technology that might now be turned more consistently to shared interests in peace and stability. Such a move would likely need a clear commitment from both governments and leading stakeholders to foster communities of practice in TIA which identify strongly with the potential gains from joint TIA for those purposes.

Across the two governments, there should be a joint policy that sets out the "threshold" at which a joint TIA would be conducted; alternately, each of the Australian and Indian governments could establish a domestic policy about TIA that references appropriate areas of interoperability as outlined above.

Australia's TIA community of practice should build on existing institutional strengths while addressing current gaps. The Critical Technologies Hub under the Department of Industry, Science and Resources (DISR) can be the nodal agency to facilitate the formation of CoPs focused on specific technology clusters (e.g., AI, quantum, biotechnology). These CoPs would bring together researchers from universities and the Commonwealth Scientific and Industrial Research Organisation (CSIRO), representatives from industry and civil society, and relevant officers from concerned government departments.

In India, our earlier paper (Austin et al 2025) noted the role played by ad hoc committees and expert groups in the conduct of TIA. However, a more structured and sustainable framework is necessary to systematically address the opportunities and risks posed by emerging technologies. One way to establish such a framework would be through the creation of a Cabinet Committee on Science and Technology (CCST), chaired by the Prime Minister. Such a high-level committee would provide political leadership and strategic direction to national efforts in technology governance. By placing TIA directly on the agenda of the highest decision-making body in government, India would signal its commitment to ensuring that technology adoption is aligned with national priorities in economic growth, security and societal well-being.

The committee could be supplemented with each interested line ministry setting up a TIA Cell that would conduct sector-specific impact assessment of emerging technologies. For example, in the Ministry of Health and Family Welfare, the adoption of digital health platforms or AI-based diagnostics requires assessments that balance innovation with patient safety and data privacy. In the Ministry of Defence, the focus would be on dual-use technologies such as autonomous systems, quantum communications or AI-enabled decision-support tools. Similarly, the Ministry of Agriculture would require impact studies on precision farming technologies, gene editing and agricultural drones.

A model structure for each TIA Cell could be to have a permanent Secretariat responsible for administrative and coordination functions, including the onboarding of experts, defining the agenda for the TIA Cell meetings, scheduling and documentation of the meetings, maintaining knowledge repositories, facilitating cross-ministerial dialogue and liaison with other government agencies. Beyond the Secretariat, each cell should draw upon a wide pool of technology and domain experts from academia, industry, and policy think tanks. At present, technology expert committees set up by the government tend to be more skewed with representation of experts from academia, since engaging with public academic institutions is seen as a safe option by the bureaucracy. This preference often results in limited engagement with industry practitioners, despite the latter frequently possessing higher domain expertise and practical experience. Also, the line departments should establish the TIA Cells as sustained communities of practice (CoP) rather than as ad hoc, topic-specific initiatives. Such continuity enables the Cells to not just provide policy recommendations informed by TIAs, but also to assess the ongoing impact of the policy measures in action. It is also important for the impact assessment conducted by these committees to be placed in the public domain to build public trust and wider scrutiny, both of which are necessary considering the rapidly evolving nature of emerging technologies.

This model ensures that each TIA Cell focuses on sectoral problems, at the same time leveraging the expertise across various segments of society, while ensuring continuity and sustenance. The Secretariat would ensure that sector-specific expertise is applied to technology assessments and ensure the building of knowledge repositories; academicians would contribute cutting-edge knowledge and methodological rigour; industry experts would bring practitioners' perspectives; and think tanks would provide perspectives on governance, ethics, and long-term societal implications.

NITI Aayog could anchor the establishment of a larger Community of Practice (CoP) that will bring together the members of the TIA Cells across the various ministries. This can be achieved through a forum where regular workshops are conducted to facilitate horizontal exchange of ideas and best practices.

This multi-layered architecture – anchored in a Cabinet Committee, executed by ministerial TIA Cells and networked through a NITI Aayog-led CoP – would give India the capacity to systematically evaluate emerging technologies. The CoP can then be leveraged for international collaborations, such as the proposed Australia–India joint TIA initiative.

4.4.1 Federated Model for Joint TIA

The Department of Foreign Affairs and Trade (DFAT) in Australia and the Ministry of External Affairs (MEA) in India would be the natural entities to anchor the joint TIA initiatives. This has to be viewed as a strategic initiative on science diplomacy, not an exercise seated in a science or industry ministry. Within DFAT, the South and Central Asia Division could take the lead in coordinating Australia's engagement, while the Oceania Division within the MEA could perform a similar role for India.

These divisions would act as diplomatic and strategic liaison points, ensuring alignment of the joint TIA efforts with broader foreign policy and geopolitical objectives. They would work in close coordination with the respective national nodal agencies responsible for Communities of Practice (CoPs), i.e. the DISR in Australia and the Office of the Principal Scientific Adviser (PSA) in India.

Through regular exchanges, the nodal divisions in DFAT and MEA could help identify shared technology domains of strategic interest. This research paper has identified a few selected domains to kick-start the joint TIA programme. The technology areas have been selected based on our assessment of complementarities in expertise and commonality in interests between the two countries. The nodal divisions could also facilitate the formation of joint working groups or thematic task forces composed of experts from both countries to co-design and co-execute TIA activities.

This federated governance model preserves institutional flexibility while enabling cross-pollination of ideas, harmonisation of assessment frameworks and sustained collaboration. It leverages diplomatic infrastructure to ensure that technical cooperation is embedded within a durable strategic partnership.

For the joint TIA initiatives to be successful and sustained, it is important for them to be supported by a strong institutional framework. Building and expanding on the current joint initiatives between the two countries, such as the Australia-India Cyber and Critical Technology Partnership (AICCTP) and the Australia-India Strategic and Technology Policy Initiative (SATPI), a formal MoU between the respective foreign affairs ministries would set up the joint TIA programme well. The MoU could define the objectives of the programme, funding availability and key principles for the partnership.

An annual summit conducted under the MoU can be a good platform for strengthening the Communities of Practice established under this programme. Beyond offering a space for networking, the summit can facilitate a meaningful exchange of ideas, showcase progress on ongoing assessments and highlight innovative policy approaches developed by both countries. It can also provide opportunities for peer learning, collaborative planning, and publication of joint reports. The summit can further act as a public-facing event, building visibility, credibility and stakeholder engagement around the bilateral collaboration.

4.5 The Strategic Advantage of a Bilateral Approach

In the current highly contested global landscape, where the constraints of complex multilateral forums are increasingly evident, a targeted bilateral approach to TIA presents several distinct advantages.

*Agility***:** Whilst multilateral forums are valuable for long-term, global-scale discussions, bilateral collaboration is conducive for dynamic scenarios that need agility. Bilateral arrangements enable swift decision-making, pilot testing and nimble adaptation, characteristics that would be difficult to achieve in broad multilateral forums where consensus is slow and diluted.

Building trust: It may also be easier to build trust when engaged bilaterally, especially in critical technology domains. With fewer participants, information sharing can be more open and comprehensive. This enhanced trust is particularly valuable in TIA, where assessments often involve sensitive information about national capabilities, strategic intentions and vulnerability assessments. The level of trust required for effective collaboration in these areas may be difficult to achieve in multilateral settings.

Tailored approach: Bilateral cooperation can be tailored to reflect the specific interests, capabilities, and institutional characteristics of the participating countries. This customisation can enhance the relevance and effectiveness of collaborative activities while accommodating each partner's unique requirements. Australia and India's shared democratic values, for example, may not be compatible with some countries that would nevertheless have a significant influence in multilateral settings. Hence, bilateral engagements can be designed to leverage each nation's strengths while addressing their specific challenges and interests.

Testbed for innovation: Bilateral cooperation allows for experimental and innovative approaches that might be difficult to implement in multilateral settings. This experimental capacity is particularly valuable in the emerging technologies domain, where methodological approaches are still evolving and novel challenges may require innovative solutions and regulatory sandboxes to assess the impact in real-world conditions.

4.6 Critical Success Factors

Four factors will be critical to the success of Australia-India TIA cooperation:

Political Commitment: Sustained political support from both countries' leaders will be essential for overcoming inertia and initial hesitancy. This support should be demonstrated through regular high-level meetings and public commitments.

Institutional Capacity: Both nations must invest in building the institutional capacity necessary for effective cooperation in TIA for peace and stability. This includes setting up the TIA Secretariat and the Communities of Practice as proposed earlier in this paper.

Resource Allocation: Adequate resources must be allocated to support cooperation activities. This includes funding for the secretariat, research activities and operational expenses. Both nations should contribute equitably to common costs.

Cultural Sensitivity: Cooperation must be conducted with sensitivity to cultural differences and institutional variations. This also requires understanding each partner's strengths, weaknesses, and organisational cultures.

4.7 Implementation Roadmap

The project recommends a joint TIA programme to be developed over three phases:

1) foundation building
2) pilot engagements
3) maturation .

In the Foundation building phase, the two countries should focus on establishing the enabling factors for successful and scalable collaboration. This includes formulating a clear bilateral policy to establish the Communities of Practice and guide joint efforts, establishing the institutional frameworks as recommended in this paper, and developing communities of practice in both countries.

The Pilot phase could involve the two countries initiating joint TIA projects in less sensitive areas to demonstrate cooperation benefits. The recently launched joint technology assessment focused on advancing maritime surveillance by Australia and India is a good example of such a domain.

The Maturation phase could see the expansion of the joint TIA programme across three dimensions.

- identifying additional technology domains to be selected for joint TIA
- expanding the collaboration to minilateral and multilateral forums
- translating the impact assessment to capacity building and national policy processes.

Capacity building would include training key stakeholders in both countries on the emerging technology ecosystem, and policy integration would see regular briefings for senior officials and policy workshops to translate the outcome of TIA process into well-informed public policy.

4.8 Selected Technologies for TIA

The potential topics which Australia and India might address in joint TIAs constitute a vast list. Our consultations produced several specific suggestions.

In the field of wireless telecommunications (5G/6G), there would be an opportunity for each country to gain from concrete TIA projects. India’s proactive stance through Mission 6G and the Bharat 6G Alliance has created a framework that includes task forces and innovation labs. Australia’s responses are largely security-driven, triggered by telecom breaches and foreign vendor risks. Joint TIA in this area could be based on opportunities for harmonizing standards, and low-cost device ecosystems – particularly involving partnerships with Indian startups.

Cybersecurity is a field identified by both countries as a high priority in official statements. Australia and India have engaged in a variety of bilateral and multilateral collaborations in this field. There is room for more focused dialogue to establish a more harmonised approach to the challenges, but joint TIA would be useful to harmonise policy in discrete areas, and to achieve greater clarity on the most beneficial paths for assessment of these technologies.

With respect to artificial intelligence and autonomous systems, there was support for the idea that the two countries could work more rigorously through joint TIA of sub-technologies to shape binding norms on responsible military uses and a regime of governance.

Another opportunity could be found in TIA in the health and biotech sectors. TIAs in India have produced formal reports, such as the rejection of BT Brinjal (genetically modified eggplant) after health and environmental concerns were analysed. Both countries might learn from the use of citizen juries in Mali or the practices of gender-responsive healthcare assessments in Latin America.

Our research team has developed three ideas for joint TIA: digital identity, pathogen detection for biosecurity, and maritime situational awareness. For advanced TIA, the projects would go beyond just technology evaluation and include governance, human rights safeguards, data sovereignty, sustainability, cultural appropriateness, and diplomatic context.

4.8.1 Joint TIA for Secure Digital Identity

Secure digital identity is the foundational layer for building robust Digital Public Infrastructure (DPI), enabling trust in digital transactions, and providing the ability to foster population-scale digital transformation. Digital identity holds even greater importance in the developing world, since it provides a means to overcome pervasive under-documentation and poor civil registration systems, which often deny citizens access to basic rights and essential public services like voting, education and government financial aid (Gelb and Clark 2013: 14n).

Secure and ethical digital identity systems can affect key security problems, including terrorist financing, human trafficking, and election security. These systems are not just technological but a political foundation for resilient, inclusive, and peaceful societies. Key technologies in play include biometric systems such as fingerprint, iris, and facial recognition; data integration for capturing and updating core personal information; and credential Issuance and authentication, such as smart cards, mobile ID solutions, and digital certificates. Models like India's Aadhaar demonstrate how a universal digital identity can be inclusive, reaching even the poorest in remote villages, and enabling efficient delivery of government subsidies, benefits and services (Indian Government UIDAI 2024).

India and Australia, both liberal democracies and committed to democratic digital governance, have adopted different approaches to implementing digital identity for their citizens. India's Aadhaar system represents a centralised and state-managed approach to digital identity, using biometrics for universal coverage and delivering large-scale public benefits efficiently (Indian Government UIDAI 2024). Whilst it has demonstrated how a single digital identity can serve as the backbone for digital governance in a developing country context, it has not been without concerns regarding potential for surveillance and exclusion (Misra 2019; Michael et al. 2019; Michael et al. 2022).

Australia, by contrast, has adopted a federated model through its Trusted Digital Identity Framework (TDIF), that envisions multiple government and private sector identity providers operating under a common set of rules (Australian Government. DTA 2024). This decentralised model relies on voluntary enrolment, user choice and high privacy standards, suitable for mature digital markets with competitive service ecosystems.

India and Australia, though, share a strategic interest in supporting the development of DPI in the Pacific Island nations (Reddy and Todi 2024). Both countries are engaged in capacity-building and technical cooperation in the region, partly motivated by the need to offer an alternative to China's growing influence through its Digital Silk Road programme under the Belt and Road Initiative.

Australia's federated identity model may be difficult to operationalise in the Pacific Islands context, where digital ecosystems are less developed, private sector identity providers are scarce, and governments may lack the institutional capacity to regulate a complex multi-provider environment. India's model, while proven and hence potentially more suited to such conditions, would need to be adapted to respect the cultural, legal and political contexts of the island countries.

In this scenario, a joint TIA by India and Australia would allow both countries to evaluate the risks, data sovereignty concerns and long-term sustainability of exporting digital identity and other DPI solutions. It would also ensure that the digital identity frameworks being promoted are inclusive, rights-respecting and technically resilient. Such TIA could also serve as a platform for India and Australia to identify the need to tailor the DPI platforms to the specific needs of small island nations, hence preventing the imposition of a one-size-fits-all model.

4.8.2 CRISPR-Based Pathogen Detection for Biosecurity

The emergence of CRISPR-based pathogen detection represents a transformative development in biotechnology. CRISPR (Clustered Regularly Interspaced Short Palindromic Repeats) is a gene-editing technology that can be adapted for highly sensitive and detection of specific pathogens. It has become very popular because of its efficiency, flexibility, and ease of use (Doudna 2014).

Several CRISPR platforms promise point-of-care testing with minimal equipment, making them suitable for use in remote, resource-limited, or crisis-afflicted areas. The technology leverages CRISPR-associated (Cas) enzymes to recognize and bind to target genetic sequences of viruses or bacteria. Upon detection, a signal is produced, indicating the presence of the pathogen. This enables rapid, low-cost diagnostics outside traditional laboratory settings.

Key technologies involved include CRISPR-associated enzymes; CRISPR RNA (ribonucleic acid) which encodes the sequence that matches the DNA (Deoxyribonucleic Acid) target; DNA Repair Pathways; Delivery Systems, such as viral vectors, electroporation, microinjection, or lipid nanoparticles that deliver CRISPR components into cells; and toolkits for modulation and control that support high precision, programmability, and broad applicability of CRISPR gene-editing systems (addgene n.d.).

This technology carries major consequences for biosecurity, public health, and global political stability. Building on past experiences with biological threats—from pandemics to bioweapons—its relevance extends beyond disease control to matters of national security and international peace. CRISPR-based diagnostics can fortify early-warning mechanisms, support outbreak management, and mitigate risks.

CRISPR diagnostics can help reduce the impact of biological warfare, thereby enhancing national and regional stability. The technology's portability and affordability improve equitable access to diagnostics. This is particularly critical during pandemics or in conflict-prone zones, where rapid containment is essential to preventing escalation.

However, dual-use risks are acute. The same tools that detect pathogens might be reverse-engineered to develop or hide bioweapons (although it could be easier/faster to use a natural pathogen as a bioweapon compared to engineering something using CRISPR). Misuse by state or non-state actors could destabilize regions or be perceived as a breach of international norms. Furthermore, improper deployment, such as through unregulated surveillance or mass screening, could erode public trust and fuel geopolitical tension.

India and Australia are both strategically placed and technically capable of evaluating CRISPR's impacts. Organisations in India such as Crisprbits, IGIB, and Swami Vivikenanda University are leading in development of platforms and tests, as are several entities in Australia.

India's Council of Scientific and Industrial Research (CSIR) has supported CRISPR tool development for infectious disease detection. Australia's Commonwealth Scientific and Industrial Research Organisation (CSIRO) similarly explores gene technologies in agriculture and public health.

Yet, comprehensive impact assessments incorporating biosecurity, peace, and dual-use implications are currently lacking in both countries. Australia has experience in risk-based regulation through its Therapeutic Goods Administration (TGA), and India is evolving its biotechnology regulatory ecosystem. Coordination between these frameworks has not been adequately exploited. There are tools available though, such as The Australia-India Strategic Research Fund (AISRF) and the Indo-Biotechnology Fund (IABF), which could be directed more to this area.

A joint Australia/India TIA would bring complementary strengths together to address strategic, scientific, and ethical dimensions of CRISPR diagnostics. This partnership could:

- develop shared biosecurity standards in the Indo-Pacific
- promote ethical frameworks to mitigate dual-use risks
- establish coordinated surveillance systems for rapid pandemic response
- lead dialogue within multilateral forums on peaceful biotech governance.

TIA collaboration would not only enhance preparedness but also contribute to peace and stability in a geopolitically sensitive region increasingly shaped by biotechnology.

4.8.3 Maritime Domain Awareness

Australia and India have expansive coastlines (35,760 km and 11,098 km respectively) and large Exclusive Economic Zones (8 million sq km and 2 million sq km). The two governments have spent substantial resources both in strategic planning and implementation of technical measures to protect their maritime borders in accordance with the law. Their mutual interest in maritime situational awareness extends to most of the Indian Ocean and its approaches, for the purposes of counter-terrorism, the protection of sea-borne commerce, monitoring of naval operations by foreign powers, and human trafficking.

Two examples of joint activities between Australia and India include AUSINDEX, a bilateral biannual naval exercise, and Exercise Malabar to “enhance maritime security and interoperability between their naval forces… crucial in countering regional threats and ensuring freedom of navigation in the Indo-Pacific” (Nath 2025:2849). The two countries also engage in air-to-air refuelling agreements and coordinated maritime patrols using manned aircraft (P-8A/P-8I Poseidon) (Varma 2025; Asia-Pacific Defence Reporter 2024).

A paper analysing the future of information and intelligence-sharing in the Indian Ocean (Brewster and Bateman 2024) identifies several recommendations for effective collaboration such as developing regional networks, supporting interoperability of platforms, developing standard operating procedures, and facilitating trust-building through joint exercises and shared systems.

For the purposes of this paper, the focus on maritime situational awareness are the technologies and processes involved in intelligence, surveillance, and reconnaissance (ISR). This is the coordinated and integrated acquisition, processing, and provision of timely, accurate, relevant, coherent, and assured information and intelligence to support national civil and military decision making.

Critical technologies involved include multi-mode sensors, AIO and machine learning, secure satcom and networks, autonomous operations, quantum and next-gen encryption, edge computing, and interoperable C2 systems. Artificial intelligence technologies are increasingly being integrated into intelligence analysis systems, as they can cope with the exponentially growing volume, velocity, and variety of data. AI could also enable autonomous vehicles to navigate independently, thereby improving surveillance capabilities.

The application of the most modern technologies can help overcome the challenges of monitoring the vastness of the Indian Ocean Region. It is next to impossible for any country, except perhaps for the US, to have stand-alone real time monitoring of the entire region. Sharing threat information between partners helps increase awareness about the broader region.

Maritime ISR is a technology area that is suitable for collaboration between India and Australia as there is convergence in interests, sensitivities are lower (as these are non-lethal applications), and there is mutual interest in stability in the Indo-Pacific region. Recent discussions between the defence establishments of both countries also highlighted cooperation priorities in maritime domain awareness, reciprocal information sharing, and industry and science and technology collaboration (Indian Government. Ministry of Defence 2025).

The cooperation at a multilateral level is well established. The Indian navy hosts the Information Fusion Centre – Indian Ocean Region (IFC-IOR), a regional maritime security centre opened in 2018. It has International Liaison Officers from 12 partner nations, including Australia. There are similar centres in other countries. The Centre publishes detailed reports on maritime situational awareness in the Indian Ocean Region on issues ranging from armed robbery and contraband smuggling to maritime security threats and climate change (IFC-IOR 2024).

Similarly, the Australian Border Operations Centre (ABOC) acts as Australia’s national information fusion centre for all civil maritime threats, collating information from stakeholders such as shipping companies and international partners. Singapore and Madagascar also operate regional information centres similar to the IFC-IOR.

Australia and India have also engaged trilaterally with Indonesia (e.g., Trilateral Maritime Security Dialogue 2025) to coordinate combined surveillance and interoperability measures across regional maritime zones (Bashfield 2025). In the broader Quad context, Australia and India, together with Japan and the US, cooperate on maritime issues related to coast guard interoperability, joint operations aboard shared platforms, and enhanced technology sharing (Hunnicutt and Brunnstrom 2024).

The first Australia-India joint TIA for peace and stability, announced in July 2025, that it is intended to improve the early detection and tracking of submarines and autonomous underwater vehicles, is a significant milestone in joint maritime domain awareness (Australian Government. Defence 2025a). This is a joint three-year research project between the Defence Science and Technology Group's (DSTG) Information Sciences Division, and its Indian counterpart agency, the Defence Research and Development Organisation's Naval Physical and Oceanographic Laboratory.

The project will explore the use of Towed Array Target Motion Analysis to improve the reliability, efficiency and interoperability of current surveillance capabilities. This involves a series of hydrophones towed behind a submarine or surface. The signals from these hydrophones will be processed algorithmically to detect acoustic signals emanating from maritime targets. This will be an additional data source that can complement existing data from satellites, drones, and open-source intelligence.

While the Towed Array Target Motion Analysis project is a great start, there is great potential for further collaboration. The adoption of new technological tools and deeper intelligence sharing cooperation between partners in the Indian Ocean Region could significantly enhance awareness.

Another joint TIA for maritime surveillance, though looking at surface operations, might focus on the coordinated use of interoperable HALE UAVs in service of both countries. The project might look to assess the interface issues that would allow Australia and India to share intelligence feeds, synchronize surveillance missions, and conduct joint maritime patrols, strengthening collective situational awareness and response. Both Australia and India have made significant investments in High-Altitude Long Endurance (HALE) Unmanned Aerial Vehicles (UAVs) for maritime surveillance, recognizing their value for persistent, wide-area intelligence, surveillance, and reconnaissance (ISR) over vast oceanic regions. As of July 2025, there is no public evidence of a formal, bilateral joint program specifically focused on the co-development, joint operation, or shared procurement of HALE UAVs for maritime surveillance between the two countries.

This project would be a natural parallel to the new project launched on 2 July 2025 for a three-year joint research project on specific technologies for sub-surface surveillance and maritime awareness (Australian Government. Defence 2025a). This project is being led by Australia's Defence Science and Technology Group's (DSTG) Information Sciences Division, and its Indian counterpart agency, the Defence Research and Development Organisation's Naval Physical and Oceanographic Laboratory.

Australia has acquired the MQ-4C Triton HALE UAV from the US (Salerno-Garthwaite 2024). This platform is now operational with the Royal Australian Air Force (RAAF) and is integrated with the P-8A Poseidon fleet for comprehensive maritime ISR. Australia's investment in HALE UAVs is projected to reach $4.7 billion over the next decade, underscoring their strategic importance for national and regional security.

India has purchased the MQ-9B SeaGuardian HALE UAV, also from the US, with a focus on persistent surveillance of the Indian Ocean Region, the Line of Actual Control, and critical maritime chokepoints (Verma 2025). The MQ-9B is seen as a force multiplier for India's maritime domain awareness and is being integrated with India's tri-service network-centric warfare systems.

Given both countries' acquisition of interoperable US-made HALE UAVs, there is a strong foundation for future operational coordination, joint exercises, or intelligence sharing using these assets (Corben et al 2025; Johnston 2025). The evolution of their partnership and the growing focus on Indo-Pacific security suggest that formal cooperation on HALE UAVs could emerge, especially within multilateral frameworks like the Quad. One challenge would be the interaction between each country's regime for technology transfer arrangements of the US-originated systems, along with data security integration between Australia and India, interoperability, and geopolitical sensitivities.

In the broader Indo-Pacific context, there are ongoing discussions and proposals for trilateral or multilateral ISR cooperation involving Australia, India, the US, and Japan. These often reference the potential for sharing HALE UAV-derived intelligence or coordinating ISR operations, but concrete Australia–India bilateral HALE UAV projects have not been reported yet.

One particularly valuable benefit of these collaborations would be to support real-time operational needs of Australia and India, not least exploitation of the international legal right of hot pursuit enshrined in the UN Law of the Sea Convention (UNCLOS). The technology class involved can be categorised as location-based services but would rely on and be improved by joint assessment of several critical technologies.

Both Australia and India are parties to UNCLOS, which under article 111 codifies the doctrine of “hot pursuit” (United Nations 1982). This provision, and subsequent references in the Convention, allow a coastal state to chase and intercept a vessel that violates its laws within any one of five maritime zones of a coastal state: internal waters, territorial sea, contiguous zone, exclusive economic zone (EEZ) or continental shelf. The right exists only so long as physical pursuit is continuous and started after giving visual or auditory warning (Article 114). The right ceases if the vessel enters the territorial waters of another state.

While the regime of hot pursuit only applies if the coastal state is in continuous physical contact with the offending foreign vessel, in many instances that continuity can only be achieved by advanced ISR assets tracking of the offending vessel (or vessels). This regime puts a premium on the most timely and highest quality of vessel tracking by all available assets, and its continuous communication to any vessels or aircraft in hot pursuit.

Scholars have discussed the potential for multilateral or bilateral frameworks to extend and cooperate on hot pursuit enforcement— addressing limitations via shared protocols, interoperable signalling, and legal coordination (Coombs 2016). Australia and India hold regular Maritime Security Dialogues, most recently in August 2024, discussing topics like Maritime Domain Awareness (MDA), search and rescue, pollution response, civil enforcement coordination, and technological sharing (Bateman 2011; Pandey 2024).

While specific bilateral technology agreements between Australia and India regarding how to satisfy art. 111 pertaining to “the right of hot pursuit” in UNCLOS (UN 1982) have not been detailed in currently available public sources, modern maritime enforcement typically employ technologies that are collectively known as “location-based services” (LBS) (Michael and Masters 2006a). Broadly speaking, LBS incorporates monitoring capabilities through satellite systems such as Global Positioning Systems (GPS) and automatic identification systems (AIS), and geographic information systems, among other capabilities.

Communication systems are necessary to transfer data between different nodes in different network types (e.g., radar network). Finally, enforcement assets are required, which may consist of maritime patrol craft such as coast guard vessels and naval ships in the water, or long-range unmanned surveillance drones or maritime patrol craft in the air. Underlying this infrastructure are information sharing platforms, allowing for near-real-time data integration, coordinated responses between various maritime forces and other national/international police, as well as joint maritime domain awareness systems.

The capabilities gained through location-based services and technologies include:

- Immediate detection and tracking of suspect vessels attempting to evade law enforcement;
- Real-time communication and procedural alignment for pursuit across contiguous and overlapping exclusive economic zones (EEZs);
- Operational readiness for high-speed coordinated intercepts supported by best-available monitoring and tracking technology (Michael and Masters 2006b).

In sum, the two countries are building the technological and operational scaffolding required for effective, internationally-recognized hot pursuit actions, relying more on shared surveillance, rapid data fusion, and interoperable platforms than on bilateral treaties specific to hot pursuit. This practical, tech-driven approach is the primary driver of enhanced cooperation in 2025 and may equally be relevant to joint undersea surveillance projects presently being organized by Australia and India.

The advantages of such a joint technology proposal include the potential for real-time threat detection by using automated signal processing and AI-driven target motion analysis when suspected enemy submarines or suspicious vessels are deemed to have violated a maritime zone; and support for the “immediacy” requirement for lawful hot pursuit. It also means that enhanced tracking and targeting can take place using next-generation sonar, machine learning for object differentiation using secure underwater communication links, allowing for precise identification, localization and persistent tracking for valid hot pursuit. All in all, this enables interoperable situational awareness and ideally may even allow for hand-offs between enforcement assets, maritime authorities and relevant police (international, regional, federal).

When countries work in a coordinated fashion and combine technological investments, the dividends are extended in the collective, making it more difficult for illegal actors to go undetected, or even exploit jurisdictional gaps that may exist. By following a rules-based approach to maritime order, technology can enhance strategies in more advanced ways using real evidence on geographic location of foreign intrusions, mitigating potential attacks in the Indo-Pacific region by implementing existing international law frameworks.

There are of course a great many challenges that present themselves when such complex endeavours are attempted. These may include:

- persistent disputes over overlapping maritime zones and contestations over sovereignty;
- varying threat perceptions between the two countries;
- the potential for UNCLOS to be implemented selectively, potentially impacting trust in the relationship;
- resource and capability gaps between Australia and India;
- operational coordination issues, such as inadequate mechanisms to gather real-time and accurate geospatial data;
- the balance in international agencies with mandates that overlap with regional and domestic actions;
- non-traditional security threats (e.g., climate-related risks) that require multidisciplinary cross-border responses (Bradford 2005);
- sovereignty sensitivities; and/or
- a lack of enforcement mechanisms and prosecution challenges.

Australia and India are enhancing hot pursuit cooperation in their maritime zones primarily by deepening technological collaboration, improving surveillance interoperability, and strengthening joint operational frameworks that underpin rapid response to maritime threats. The trend in maritime security across the board is towards coordinated, information-driven operations, even though in the case of hot pursuit it is only vessels of the coastal state that can undertake the physical action against an offending vessel.

5. Potential of a Multilateral Approach to TIA

Bilateral cooperation can serve as a testing ground for approaches that might later be scaled up to minilateral and potentially even to multilateral forums. By developing tested methodologies, analytical tools and compatible institutional structures, bilateral partners can create the foundation for expanded cooperation. Successful bilateral cooperation can demonstrate the effectiveness of joint TIA efforts and encourage other nations to participate in expanded multilateral arrangements. By producing valuable analytical outputs and demonstrating effective collaboration, bilateral partners can build confidence in cooperative approaches to technology assessment.

Australia-India TIA cooperation could also contribute to broader regional integration by demonstrating the value of technology cooperation and building confidence in joint approaches to emerging challenges. This could support the development of regional technology governance frameworks and contribute to Indo-Pacific stability.

Australia-India bilateral TIA in certain domains could potentially roll up to the Quad. The insights and methodologies developed through the bilateral partnership could be shared within the Quad's Critical and Emerging Technology Working Group, enriching its work and strengthening its effectiveness.

It could also serve as a model for broader forums such as Indian Ocean Rim Association and Indo-Pacific Economic Framework. Development of a common understanding and a shared approach to the governance of emerging technologies could also enable Australia and India to play a more influential role in shaping global norms and standards in forums, such as the United Nations.

In this way, the bilateral partnership would not be an alternative to multilateralism, but a vital building block for a more effective and inclusive global technology governance architecture. It would also enable the two countries to play a stronger role in minilateral and multilateral forums.

Australia and India might promote more joint TA at the multilateral level, which would produce greater diplomatic gains for both countries, especially if limited to the developing countries of the Indian and Western Pacific, and if focused on sub-technologies of AI relevant to development and social stability. Few developing countries have the resources to create policy affecting peace and stability in most areas of critical technology.

Australia and India can take a lead in institutionalising innovative approaches and commitment to the enactment of a community of practice forming natural relationships at the grassroots and spurring on impactful outcomes across diverse networks, incorporating representative stakeholders, inclusive of citizen participation and the third sector.

6. Conclusion

There are bright prospects for bilateral joint TIA between Australia and India on critical technologies affecting peace and stability. Yet we also assess that the number of actual cases where the bilateral approach might be justified would be small, likely in the range of one to three per year. On the other hand, the cases where Australia and India might promote more joint TIA at the multilateral level would produce greater diplomatic gains for both countries, especially if limited to plurilateral groupings of the developing countries of the Indian Ocean region and the Western Pacific and if focused on sub-technologies of AI relevant to development and social stability. Few developing countries have the resources to create policies affecting peace and stability in most areas of critical technology.

Australia and India can take a lead in institutionalising innovative approaches and commitment to the enactment of a community of practice, forming natural relationships at the grassroots, and spurring on impactful outcomes across diverse networks, incorporating representative stakeholders, inclusive of citizen participation and the third sector. There appears to be considerable room and escalating demand for joint TIAs involving Australia and India at the bilateral and minilateral levels, such as the Quad.

It is not often in international relations that a tool for managing domestic policy (in this case, TIA) becomes widely accepted as an important and useful mechanism for managing big problems of peace and international stability. We have seen in the examples of the Five Eyes and NATO how important joint technology assessments could be in helping build cohesion and confidence among states facing severe security challenges. We also observed that states undergoing heightened tensions with a potential adversary have been able to use this tool to good effect to reduce tensions.

Our research has shown that joint TIA at the international level, whether multilateral or bilateral, is above all else a geopolitical undertaking. This reality influences the way in which states pursue such joint assessments, but there are numerous cases where heightened tensions have not prevented meaningful confidence building work on matters of critical technology affecting peace and stability.

In the first half of 2025, political unpredictability in US policy has created considerable uncertainty about continuity of US involvement in multilateral and bilateral forums, including on TIA of critical technologies. Both Australia and India are currently dealing with this US-originated uncertainty. The longer the uncertainty persists, the more Australia and India may need to back-pedal on the potential for joint TIA in the framework of the Quad.

At the same time, Australia and India do not share exactly parallel approaches to countries like China and Russia, which are seen as pursuing technological supremacy in ways that seriously challenge Australian and Indian interests. Despite dispositions in Australia and India to exclude China from sensitive technology arrangements, there are still reasonable foundations for collaboration among these countries on urgent global security issues, especially mitigating climate change and preventing another pandemic.

There is a broad international consensus that global peace and stability are potentially threatened by unregulated use of artificial intelligence, on such a scale as to command the same sort of collaborative approaches that Australia, India and China have been undertaking in a range of multilateral forums, not least in respect of climate change. There is an emerging view that joint technology assessments of sub-technologies in the field of artificial intelligence are worthy of global common approaches on responsible use that dictate putting aside, as far as possible, the sorts of geopolitical tensions that Australia and India both experienced in their relations with China.

Beyond AI, similar considerations apply across the spectrum of emerging technologies such as quantum computing, synthetic biology, 6G, and space technologies. Each of these carries transformative potential, but also profound risks if deployed without adequate multilateral safeguards, ethical frameworks, or international coordination.

Just as in the case of AI, joint technology impact assessments in these fields can provide a means to anticipate unintended consequences for peace and stability, to mitigate associated risks and to shape norms that could transcend geopolitical rivalries. Australia and India, as leading liberal democracies and with common interests in fostering international peace and stability, are well-positioned to start exploring bilateral partnerships for such joint assessments. A key departure point will be their leadership in developing much stronger communities of practice at the bilateral and regional level

TIAs are no longer a niche regulatory tool; they represent the scaffolding on which peaceful technological futures are built. The experiences, insights, and proposals captured through this dialogue reveal how joint assessments, when done right, can harmonise governance, uplift communities, and reduce geopolitical friction. Australia and India, by leveraging their respective strengths and aligning missions, are poised to become global champions of ethical and inclusive technological progress.

.

References[1]

3GPP (2024) 'SA WG3 (Security and Privacy)' 3rd Generation Partnership Project, https://www.3gpp.org/3gpp-groups/service-system-aspects-sa/sa-wg3

addgene (n.d.) 'Crispr Guide', https://www.addgene.org/guides/crispr/

AGARD (1978) 'The AGARD Propulsion and Energetics Panel: 1952–1977', AGARD-AG-215, Propulsion and Energetics Panel, NATO Advisory Group for Aerospace Research and Development, https://apps.dtic.mil/sti/tr/pdf/ADA063849.pdf

AI Now Institute (2025) 'Artificial Power: 2025 Landscape Report', https://ainowinstitute.org/publications/research/1-1-the-agi-mythology-the-argument-to-end-all-arguments

Salerno-Garthwaite A (2024) 'Australia welcomes first MQ-4C Triton to enhance maritime surveillance', Airforce Technology , 20 June, https://www.airforce-technology.com/news/australia-welcomes-first-mq-4c-triton-to-enhance-maritime-surveillance/

ARPANSA (2024) 'Australian National Report to the Joint Convention Eighth Review Meeting', Australian Radiation Protection and Nuclear Safety Agency, https://www.arpansa.gov.au/sites/default/files/documents/2024-08/Australian%20National%20Report%20to%20the%20Joint%20Convention%20Eighth%20Review%20Meeting%20-%20August%202024_0.pdf

Asia-Pacific Defence Reporter (2024) 'MQ-4C Triton to improve Australia's maritime surveillance', https://asiapacificdefencereporter.com/mq-4c-triton-to-improve-australias-maritime-surveillance/

Austin G, Bappanad K, Henry, Michael K, Materano L, Reddy B, Walker-Munro B, Withers G (2025) Technology Impact Assessment for Peace and Stability: A Comparative Study on Australia and India, Social Cyber Institute, https://www.socialcyber.co/_files/ugd/15144d_c5acc66a4a014035a939a1b534f06822.pdf

Australian Government. Defence (2024) 'AUKUS trials artificial intelligence in robotic vehicles', Defence News, 6 February, https://www.defence.gov.au/news-events/news/2024-02-06/aukus-trials-artificial-intelligence-robotic-vehicles

Australian Government. Defence (2025a). 'Indian pact bolsters undersea surveillance'. Available at: https://www.defence.gov.au/news-events/news/2025-07-03/indian-pact-bolsters-undersea-surveillance

Australian Government. Defence (2025b) "Travel to South and Southeast Asia", 1 June, https://www.minister.defence.gov.au/media-releases/2025-06-01/travel-south-southeast-asia

Australian Government. Defence (2025c) 'India's Chief of Defence Staff General Anil Chauhan's first visit to Australia', 6 March, https://www.defence.gov.au/news-events/releases/2025-03-06/indias-chief-defence-staff-general-anil-chauhans-first-visit-australia

Australian Government. Defence.(2025d) '9th Australia-India Defence Policy Talks', 18 March, https://www.defence.gov.au/news-events/releases/2025-03-18/9th-australia-india-defence-policy-talks

Australian Government. Defence (2025e) 'Address: Australia India Institute Trilateral Maritime Security Dialogue', https://www.minister.defence.gov.au/speeches/2025-06-24/address-australia-india-institute-trilateral-maritime-security-dialogue (Accessed: 14 July 2025).

Australian Government. DISR (2025) '$4 million for cutting-edge science research projects in Australia and India', 10 February, Department of Industry, Science and Resourceshttps://www.industry.gov.au/news/4-million-cutting-edge-science-research-projects-australia-and-india

Australian Government. DISR (n.d.). "Collaborating with India on science and research", Department of Industry, Science and Resources, https://www.industry.gov.au/science-technology-and-innovation/international-collaboration/collaborating-india#australiaindia-strategic-research-fund-1

Australian Government. DTA (2024) 'Trusted Digital Identity Framework', Digital Transformation Agency, https://architecture.digital.gov.au/trusted-digital-identity-framework-tdif-0

Australian Submarine Agency (2024) 'Locations for nuclear waste storage and disposal — FOI Disclosure Documents (ASA-FOI-035_23_24)', https://www.asa.gov.au/node/51

[1] References are cited according to the Australian Government Style Manual, with minor adaptations.

Barnes A (2020) 'How Canada's intelligence agencies helped keep the country out of the 2003 Iraq war, Open Canada', 18 November, https://opencanada.org/how-canadas-intelligence-agencies-helped-keep-the-country-out-of-the-2003-iraq-war/

Bashfield S (2025) 'Trilateral Maritime Security Dialogue 2025: Australia, India, and Indonesia', Australia India Institute, https://aii.unimelb.edu.au/wp-content/uploads/2025/04/Trilateral-Maritime-Security-Dialogue-2025-Brief-1.pdf

Bateman S (2011) 'Solving the "Wicked Problems" of Maritime Security: Are Regional Forums up to the Task?', Contemporary Southeast Asia, vol. 33, no. 1, pp. 1–28, https://www.jstor.org/stable/41288813

Becker C, ten Oever N, Nanni R (2024) 'Interrogating the standardisation of surveillance in 5G amid US–China competition', Information, Communication & Society, https://doi.org/10.1080/1369118X.2024.2302991

Bojić L, Djukanović D, and Nikolić N (2021) '5G as Geopolitical Power Struggle: The New Neutral Approach of Balance and Safety in Technology Controlled World Explained through a Case Study of Serbia', . NBP. Nauka, bezbednost, policija, 26(3), 25–47, https://doi.org/10.5937/nabepo26-32214

Boycott O (2014) 'Five Eyes' surveillance pact should be published, Strasbourg court told', The Guardian, 9 September, https://www.theguardian.com/world/2014/sep/09/five-eyes-surveillance-pact-appeal-disclosure-human-rights

Bradford J F (2005) 'The Growing Prospects of Maritime Security Cooperation in Southeast Asia', Naval War College Review, vol. 58, no. 3, pp. 63-86, https://apps.dtic.mil/sti/tr/pdf/ADA522808.pdf

Brewster D and Bateman S (2024) 'Maritime Domain Awareness 3.0', National Security College, Australian National University, https://nsc.anu.edu.au/sites/default/files/2024-09/Maritime%20Domain%20Awareness%203.0%20Report%202024.pdf

Bruer A and Brake D (2021) 'Mapping the International 5G Standards Landscape and How It Impacts U.S. Strategy', Information Technology and Innovation Foundation, https://itif.org/publications/2021/11/08/mapping-international-5g-standards-landscape-and-how-it-impacts-us-strategy/

Chacko P and Wilson J (2020) 'Australia, Japan and India: A trilateral coalition in the Indo-Pacific?', Perth USAsia Centre, https://perthusasia.edu.au/research-and-insights/publications/australia-japan-and-india-a-trilateral-coalition-in-the-indo-pacific/

Chow M C and Ma M (2022) 'A Secure Blockchain-Based Authentication and Key Agreement Scheme for the 3GPP 5G Network', Frontiers in Communications and Networks, 3, Article 9229231. https://pmc.ncbi.nlm.nih.gov/articles/PMC9229231/

CISA (2021) 'Iranian Government-Sponsored APT Cyber Actors Exploiting Microsoft Exchange and Fortinet Vulnerabilities in Furtherance of Malicious Activities', Cybersecurity and Infrastructure Security Agency, 19 November, https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-321a

CISA, FBI, NSA, ASD, CCCS, NCSC-NZ and NCSC-UK (2024) 'PRC State-Sponsored Cyber Activity: Actions for Critical Infrastructure Leaders', https://www.cisa.gov/sites/default/files/2024-03/Fact-Sheet-PRC-State-Sponsored-Cyber-Activity-Actions-for-Critical-Infrastructure-Leaders-508c_0.pdf

CISS (Center for International Security and Strategy) (2024) 'China-U.S. Track II Dialogue on Artificial Intelligence Interim Report', Tsinghua University, https://ciss.tsinghua.edu.cn/info/banner/7041

Congressional Research Service (2024) 'AUKUS Pillar 2 (Advanced Capabilities): Background and Issues for Congress', R47599, https://www.congress.gov/crs-product/R47599

Coombs CT (2016) 'The Doctrine of Hot Pursuit under International Law', Faculty of Law, The University of Western Australia, https://api.research-repository.uwa.edu.au/ws/portalfiles/portal/20466444/THESIS_DOCTOR_OF_PHILOSOPHY_COOMBS_Caroline_2016.pdf

Corben T, Johnstone C B, Dean P, Kotani T (2025) 'A partnership for the AJUS: Operationalising Australia-Japan-United States defence cooperation', United States Studies Centre, https://www.ussc.edu.au/a-partnership-for-the-ajus-operationalising-australia-japan-united-states-defence-cooperation

DHS (Department of Homeland Security) (2020) 'AUDREY Hastings experiment: After action report', (DHS S&T Publication No. 20-23854). in association with Defence Research and Development Canada Centre for Security Science, https://www.dhs.gov/sites/default/files/publications/2020_050620_st_ahe_aar.pdf

Die Y (2025) 'Research on the Roadmap and Prospect of BRICS Cooperation Mechanism from the Perspective of BRICS Committed to Innovation', Journal of International Economy and Global Governance, *2*(3), 3-20, https://www.mospbs.com/uploads/files/2025/05/20250508/c551b550725fb68d2af42d3ddd94c14d.pdf

Doudna J A and Charpentier E (2014) 'The new frontier of genome engineering with CRISPR-Cas9', Science, 346(6213), 1258096, doi:10.1126/science.1258096, https://www.science.org/doi/10.1126/science.1258096

EastWest Institute. (2009). "Iran's Nuclear and Missile Potential A Joint Threat Assessment by U.S. and Russian Technical Experts", https://fsi9-prod.s3.us-west-1.amazonaws.com/s3fs-public/Holloway_Hecker_EastWest_Institute.pdf

European Commission (2024) 'Communication from the Commission to the European Parliament and The Council Advancing European Economic Security: An Introduction to Five New Initiatives', 24 January, COM(2024) 22 final, https://commission.europa.eu/system/files/2024-01/Communication%20on%20European%20economic%20security.pdf

European Commission (2025) 'Communication from the Commission to the European Parliament and the Council: Quantum Europe Strategy: Quantum Europe in a Changing World', 2 July, COM(2025) 363 final, eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX%3A52025DC0363

European Commission and Quantum Flagship (2024) 'Strategic Research and Industry Agenda', https://qt.eu/media/pdf/Strategic-Reseach-and-Industry-Agenda-2030.pdf

EPRS (2014) 'The ECHELON Affair: The EP and the global interception system 1998 - 2002', European Parliamentary Research Service, https://historicalarchives.europarl.europa.eu/files/live/sites/historicalarchive/files/03_PUBLICATIONS/03_European-Parliament/01_Documents/the-echelon-affair-en.pdf

Gelb A and Clark J (2013) 'Identification for Development: The Biometrics Revolution', Working Paper 315. Center for Global Development, https://www.cgdev.org/sites/default/files/1426862_file_Biometric_ID_for_Development.pdf

Henry S, Alsohaily A, and Sousa E (2020) 'Evaluating the Compliance of the 3GPP 5G New Radio System with the ITU IMT-2020 Requirements', *IEEE Access*. arXiv pre-print: https://arxiv.org/abs/2004.00366, DOI: https://doi.org/10.1109/ACCESS.2020.2977406

Herzog S and Kunertova D (2024) 'NATO and Emerging Technologies—The Alliance's Shifting Approach to Technology Assessment and Innovation', *Naval War College Review*, 77(2), https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=8417&context=nwc-review

Hunnicutt T and Brunnstrom D (2024) 'Quad group expands maritime security cooperation at Biden's farewell summit', Reuters, Updated September 23, 2024, https://www.reuters.com/world/quad-expand-maritime-security-cooperation-bidens-farewell-summit-2024-09-21/

IBM Quantum (2025) Growing the global quantum ecosystem, Quantum Research Blog, 11 March, https://www.ibm.com/quantum/blog/japanese-quantum-ecosystem

ICAO (2018) 'Risk Assessment Manual for Civil Aircraft Operations over or Near Conflict Zones' (Doc 10084, 3rd edition). International Civil Aviation Organisation. https://www.icao.int/sites/default/files/Security/SFP/Documents/Doc.10084.Third-edition.pdf

IFC-IOR (2024) 'Annual Report 2024', The Information Fusion Centre – Indian Ocean Region, https://ifcior.indiannavy.gov.in/themes/custom/ifc_ior/static/img/2025/Annual_report.pdf

Imbrie A and Kania, E B (2024) 'AI Safety, Security and Stability Among the Great Powers', CSET Policy Brief, Georgetown University, Center for Security and Emerging Technology, https://cset.georgetown.edu/wp-content/uploads/CSET-AI-Safety-Security-and-Stability-Among-the-Great-Powers.pdf

Indian Government. Ministry of Defence (2025) '9th India-Australia Defence Policy Talks held in New Delhi', 17 March, https://www.pib.gov.in/PressReleasePage.aspx?PRID=2111839

Indian Government. UIDAI (2024) 'Annual Report 2023-24', Unique Identification Authority of India, https://uidai.gov.in/images/2023-24_Final_English_Final.pdf

James P (2023) 'NATO Harnesses Quantum Technologies for Euro-Atlantic Security: Aims for Quantum-Readiness by 2030', 4 December, https://quantumzeitgeist.com/nato-quantum-technologies-defence/

Johnston P (2025) 'Converging Currents: A case for enhanced Australia-India-US maritime intelligence sharing and security cooperation in the Indian Ocean', United States Studies Centre, https://www.ussc.edu.au/a-case-for-enhanced-australia-india-us-maritime-intelligence-sharing-and-security-cooperation-in-the-indian-ocean

Lacey S (2020) 'Huawei's window of opportunity closes: how geopolitics triumphed over technology', The Conversation, 8 July, https://theconversation.com/huaweis-window-of-opportunity-closes-how-geopolitics-triumphed-over-technology-142158

Layton P (2023) 'The Deepening Australia–India Geostrategic Relationship', Contemporary Issues in Air and Space Power, 1(1), https://ciasp.scholasticahq.com/article/83219-the-deepening-australia-india-geostrategic-relationship

Lee J, Nouwens M, and Tay K-L (2022) ‘Strategic Settings for 6G: Pathways for China and the US’, International Institute for Strategic Studies, https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/2022/08/strategic-settings-for-6g-pathways-for-china-and-the-us.pdf

Lipford M, Guirguis I, Jha S, Cichonski J (2025) “3GPP shifts focus toward 6G while continuing work on 5G-advanced”, Urgent Communications, 3 June, https://urgentcomm.com/public-safety/3gpp-shifts-focus-toward-6g-while-continuing-work-on-5g-advanced

Lord Ismay (1954) ‘NATO The First 5 Years 1949-1954’, NATO, https://archives.nato.int/uploads/r/null/2/1/216977/NATO-The_first_5_years_1949-1954__by_Lord_Ismay_.pdf

MacLeod R (1994) ‘“All for Each and Each for All”: Reflections on Anglo-American and Commonwealth Scientific Cooperation, 1940–1945’, *Albion*. 1994;26(1):79-112. https://doi.org/10.2307/4052100

Michael K (2025) Technology Impact Assessment for Peace and Stability, TIA Series: Interviews, Australia India Cyber and Critical Technologies Partnership (AICCTP), https://www.youtube.com/watch?v=e0brGlY-NnI&list=PLg4RQrKJML2uE3lEmT1-I9UWwrs8dKiBH

Michael K and Masters A (2006a) ‘Realized applications of positioning technologies in defense intelligence’, in Hussein A Abbass and Darryl Essam (eds) *Applications of Information Systems to Homeland Security and Defense*, Idea Group Publishing, pp. 167-195

Michael K and Masters A (2006b) ‘The advancement of positioning technologies in defense intelligence’, in Hussein A. Abbass and Darryl Essam (eds), *Applications of Information Systems to Homeland Security and Defense*, Idea Group Publishing, pp. 196-220

Michael K, Abbas R, Jayashree P, Bandara R J, Aloudat A (2022) ‘Biometrics and AI Bias’, IEEE Transactions on Technology and Society, vol. 3, no. 1, pp. 2-8, March 2022, doi: 10.1109/TTS.2022.3156405

Michael K, Kobran S, Abbas R, Hamdoun S (2019) ‘Privacy, Data Rights and Cybersecurity: Technology for Good in the Achievement of Sustainable Development Goals’, 2019 IEEE International Symposium on Technology and Society (ISTAS), Medford, MA, USA, 2019, pp. 1-13, doi: 10.1109/ISTAS48451.2019.8937956

Misra P 2019 ‘Lessons from Aadhaar: Analog aspects of digital governance shouldn’t be overlooked’, Pathways for Propserity Commission, https://pathwayscommission.bsg.ox.ac.uk/sites/default/files/2019-09/lessons_from_aadhaar.pdf

Nath G K (2025) ‘Autonomy and Cooperation: India's Engagement in The Indo-Pacific’, *International Journal of Social Science and Human Research*, vol. 8, 2846-2852, https://doi.org/10.47191/ijsshr/v8-i5-25

NATO (2024) ‘Environment, climate change and security’, 18 July, https://www.nato.int/cps/en/natohq/topics_91048.htm

NATO Archives (n.d.) ‘Series AC/274 - Committee on the Challenges of Modern Society (CCMS)’, https://archives.nato.int/committee-on-challenges-of-modern-society-ccms

NATO Project SPS G9895 (n.d.) Secure Communication via Classical and Quantum Technologies, https://www.quantum-safe-cryptography.science/home

OECD (2024a) ‘OECD and UN announce next steps in collaboration on Artificial Intelligence’, Organisation for Economic Co-operation and Development, 22 September, https://www.oecd.org/en/about/news/press-releases/2024/09/oecd-and-un-announce-next-steps-in-collaboration-on-artificial-intelligence.html

OECD (2024b) ’Assessing Potential Future Artificial Intelligence Risks, Benefits and Policy Imperatives’, OECD Artificial Intelligence Papers, No. 15. Organisation for Economic Co-operation and Development, https://www.oecd.org/en/publications/assessing-potential-future-artificial-intelligence-risks-benefits-and-policy-imperatives_3f4e3dfb-en.html

OECD (2024c) ‘Defining AI Incidents and Related Terms’, OECD Artificial Intelligence Papers, No. 24. Organisation for Economic Co-operation and Development, https://www.oecd.org/en/publications/oecd-artificial-intelligence-papers_dee339a8-en.html

OECD (2025) ‘Towards a Common Reporting Framework for AI Incidents’, OECD Artificial Intelligence Papers, No. 34. Organisation for Economic Co-operation and Development, https://www.oecd.org/en/publications/towards-a-common-reporting-framework-for-ai-incidents_f326d4ac-en.html

Pandey P (2024) ‘India-Australia Maritime Cooperation: Strengthening a Robust Partnership in the Indo-Pacific’, Indian Council of World Affairs, 30 August, https://www.icwa.in/show_content.php?lang=1&level=3&ls_id=11720&lid=7128

QUIN Quantum Center of Excellence (2024) ‘Quantum Science & Technology in the QUAD Nations Landscape and Opportunities’, https://psa.gov.in/CMS/web/sites/default/files/psa_custom_files/QUIN_Quantum_CoE_Report_Final.pdf

Rachman V H (2025) 'Global Geopolitical Dynamics: BRICS' Collective Strategy in Facing Western Domination and Its Implications for Indonesia', *Jurnal Ilmiah Multidisiplin Indonesia (JIM-ID)*, 4(4), 117-128, https://ejournal.seaninstitute.or.id/index.php/esaprom/article/download/6561/5058/17748

Reddy B (2023) 'Open RAN: Challenges and Pathways for Adoption', 24 September, https://takshashila.org.in/research/open-ran-challenges-and-pathways-for-adoption

Reddy B and Todi S (2024) 'India-Australia collaboration on digital public infrastructure in the Pacific', The Strategist, 4 March, https://www.aspistrategist.org.au/india-australia-collaboration-on-digital-public-infrastructure-in-the-pacific/

Retzmann N (2025) 'Narratives of Competition, Competition of Narratives? United States–China Relations, Technology, and the Role of Storytelling', https://academic.oup.com/isagsq/article/5/2/ksaf036/8119779

Rühlig T (2021) 'The Shape of Things To Come: The Race to Control Technical Standardisation', European Chamber, December 2021, https://static.europeanchamber.com.cn/upload/documents/documents/The_Shape_of_Things_to_Come_English_Final%5b966%5d.pdf

Schmid G (2001) 'Report on the existence of a global system for the interception of private and commercial communications (ECHELON Interception System) (A5-0264/2001) European Parliament Temporary Committee Report and Resolution, European Parliament, Temporary Committee on the ECHELON System, July 2001, https://www.europarl.europa.eu/doceo/document/A-5-2001-0264_EN.html

Schmitt P (2024) ;3GPP Standardization', 3GPP, https://www.3gpp.org/ftp/Information/presentations/Presentations_2024/02_3GPP-Standardisation.pdf

Sevilla J, Heim L, Ho A, Besiroglu T, Hobbhahn M, Villalobos P (2022) 'Compute Trends across Three Eras of Machine Learning', https://arxiv.org/pdf/2202.05924

Siddiqui s, Loke K, Clare S, Lu M, Richardson A, Ibrahim L, McGlynn C, Ding J (2025) 'Promising Topics for US–China Dialogues on AI Governance and Safety', CSET Research Report, Georgetown University, https://oms-www.files.svdcdn.com/production/downloads/academic/Final%20Promising%20Topics%20for%20US-China%20Dialogues%20on%20AI%20Governance%20and%20Safety.pdf?dm=1737452069

Swayne M (2024) 'Report: China and Russia Test Quantum Communication Link', Quantum Insider, 9 May, https://thequantuminsider.com/2024/01/02/report-china-and-russia-test-quantum-communication-link/

The White House (2025) 'Winning the Race America's AI Action Plan', July, https://www.whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf

Turchetti S (2010) 'NATO: Cold-warrior or eco-warrior', Research Europe, 28 October, reprinted in 'Science & the Alliance NATO's Third Dimension: Supplementary articles', https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2014_12/20150225_1412-Brochure_Science_2_Suppl.pdf

UNCTAD (2022) 'COVID-19 and Maritime Transport: Impact and Responses: Navigating the Crisis and Lessons :Learned', United Nations Conference on Trade and Development, UNCTAD/DTL/INF/2022/1, https://unctad.org/system/files/official-document/tcsdtlinf2022d1_en.pdf

United Nations (1982) 'United Nations Convention on the Law of the Sea', https://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf

Verma R (2025) 'HALE over MALE: Why India's MQ-9B procurement may redefine its UAV doctrine', Indian Aerospace Defence Bulletin, 3 May, https://www.iadb.in/2025/05/03/hale-over-male-why-indias-mq-9b-procurement-may-redefine-its-uav-doctrine/

Wenger-Trayner E and Wenger-Trayner B (2015) 'Introduction to communities of practice', https://www.wenger-trayner.com/introduction-to-communities-of-practice/

WHO (2025) 'WHO COVID-19 Technology Access Pool', World Health Organisation, https://www.who.int/initiatives/covid-19-technology-access-pool

World Privacy Forum (2024) 'How Canada's Algorithmic Impact Assessment Process and Algorithm Has Evolved', AI Governance on the Ground Series, August 2024, https://worldprivacyforum.org/documents/9/WPF_AI_Governance_Canada_AIA_August2024_fs.pdf

Zhang B and Allen G C (2024) 'U.S.-China AI Safety Dialogue: Terminology and Risk Consensus', *ACM Digital Library*, https://dl.acm.org/doi/full/10.1145/3715275.3732080

Appendix 1: Supplementary Bibliography: Notable TIA Studies and Reports 2022-2025

Australian Government. Digital Transformation Agency (2025) ‘Major Digital Projects Report 2025: Technology Assessment and Oversight’, https://www.digital.gov.au/sites/default/files/documents/2025-03/2025%20Major%20Digital%20Projects%20Report.pdf

Casaburo D, Jarlsbo M, Lückerath D, Normelli (2024) ‘Assessing AI Technologies for LEA Use: The ALIGNER Methodology’, Gkotsis I, Kavallieros D, Stoianov N, Vrochidis S, Diagourtas D, Akhgar, B (eds), *Paradigms on Technology Development for Security Practitioners*, pp. 225-235, Cham: Springer Nature Switzerland

Grunwald, A. (ed.). (2024). *Handbook of Technology Assessment*. Edward Elgar Publishing.https://www.e-elgar.com/shop/gbp/handbook-of-technology-assessment-97810353

Hennen L, Hahn J, Ladikas M, Lindner R, Peissl W, van Est R (eds) (2023). *Technology Assessment in a Globalized World: Facing the Challenges of Transnational Technology Governance*. Springer International Publishing, https://library.oapen.org/handle/20.500.12657/60800

Kop M (2023) ‘Quantum technology impact assessment’, *EU AI Alliance,* European Commission, April, https://futurium.ec.europa.eu/en/european-ai-alliance/best-practices/quantum-technology-impact-assessment

OECD (2023) ‘Technology Assessment for Emerging Technology: Case Studies and Principles’, https://www.oecd-ilibrary.org/science-and-technology/technology-assessment-for-emerging-technology_e738fcdf-en

OECD (2023) ‘Technology Assessment for Emerging Technology: Meeting New Demands for Strategic Intelligence’. *OECD Science, Technology and Industry Policy Papers*, https://www.oecd-ilibrary.org/science-and-technology/technology-assessment-for-emerging-technology_e738fcdf-en

U.S. Department of Defense (2023) ‘Critical Technology Elements and Technology Readiness Levels: Technology Readiness Assessment Guidebook’, https://www.cto.mil/wp-content/uploads/2023/07/TRA-Guide-Jun2023.pdf

U.S. Department of Defense (2023) ‘Options for Addressing Immature Critical Technology Elements: Technology Readiness Assessment Guidebook’, https://www.cto.mil/wp-content/uploads/2023/07/TRA-Guide-Jun2023.pdf

UNCTAD (2025) ‘Technology and Innovation Report 2025: Inclusive Artificial Intelligence for Development. United Nations Conference on Trade and Development’, https://unctad.org/system/files/official-document/tir2025_en.pdf

Appendix 2: Contributing Authors and Team Members

Professor Greg Austin is a Director of the Social Cyber Institute. He has held appointments in the International Relations Department at ANU, the International Institute for Strategic Studies (IISS), the Department of War Studies King's College London, and the University of New South Wales in Canberra. He is also currently an adjunct Professor at the University of Technology Sydney. Austin has worked on technology assessment for military and strategic purposes from social science perspectives, including consultancies for the UK, Japanese and Australian governments. His perspectives on technology assessment have been outlined in his short report authored for IISS, "Quantum Sensing: Comparing the United States and China" (2024). Austin was co-editor and contributing author for the IISS two-part series on "Cyber Capabilities and National Power" (2021 and 2023). He has published two books on China's cyber power, an additional eight books on international security, and numerous articles and reports in the same fields.

Karthik Bappanad, the co-chief investigator with Professor Withers, is a technologist with a keen interest in public policy, and currently a consultant at InKlude Labs, based in Bengaluru India. Karthik was earlier heading CySecK, Karnataka state's Centre of Excellence in Cyber Security, prior to which he was heading Security Engineering at ReBIT. He likes to work in the intersection of technology, policy and ethics. InKlude Labs is a research and consulting organisation, focusing on areas that have an impact on policy and governance. Inklude Labs has considerable experience, including under an existing AICCTP Round 3 grant, in delivering advanced research and related public policy activities along with conducting educational outreach on public policy.

Adam P. Henry is a Senior Fellow in the Social Cyber Institute and a Partner in the Social Cyber Group. He is a policy and programme specialist in cyber security education, skills and workforce development. He has instigated key pilot programmes that are focused on growing and developing the required multifaceted multidisciplinary cyber skills within the economy. He was invited to participate as a subject matter expert in the 2017 Prime Minister's Cyber Taskforce, and has been invited to brief ministers, shadow ministers and government senior executives on these key topics to develop cyber strategies and initiatives. He has provided key research papers on cyberspace and has been fortunate to be invited globally to speak on these key topics. He has had a broad cyberspace professional career spanning the Australian Public Service, a major consulting firm, academia, working in multiple startups, his own consulting business and industry accelerators and clusters. Adam is undertaking doctoral studies at the RMIT University where he also facilitates post graduate studies in cyber security, digital and AI.

Pranay Kotasthane is the deputy director at the Takshashila Institution and chairs its High-Tech Geopolitics Programme. He teaches public policy, international relations and public finance and is a co-author of popular books on public policy like 'Missing in Action', 'When the Chips are Down' and 'We, the Citizens'.

Lisa Materano is the Chief Executive Officer, Blended Learning International and a Director of the Social Cyber Group. Lisa Materano is a dynamic leader with extensive expertise in education, training, and strategic partnerships. As CEO of Blended Learning International (BLI) and Director of the Social Cyber Group (SCG), she drives innovative programmes in professional development, accredited education, and cyber-focused initiatives. Lisa has spearheaded projects with a global focus, including pathways development under the Australian Qualifications Framework (AQF) and international collaborations such as online course delivery in India and tailored presentations to Chinese delegations. Her leadership reflects a commitment to excellence and a vision for equipping professionals with future-ready skills. In this project, Lisa's strategic insight and passion for impactful education ensure alignment with industry needs and sustainable growth, leveraging her proven expertise in cross-cultural engagement and organisational development.

Katina Michael (Senior Member, IEEE) received the B.S. degree in information technology from the University of Technology Sydney in 1996, the Doctor of Philosophy degree from the University of Wollongong Australia in 2003, and the Master of Transnational Crime Prevention degree from the University of Wollongong in 2009. She researches the social, legal, and ethical implications of emerging technologies. She is presently a Visiting Research Scientist at Arizona State University where she was a joint tenured professor 2018-2024 for the School for the Future of Innovation in Society and the School of Computing and Augmented Intelligence, and where she also directed the Society Policy Engineering Collective. She is the Founding Editor-in-Chief of the *IEEE Transactions on Technology and Society* and a board member of the Australian Privacy Foundation.

Bharath Reddy is an Associate Fellow with the High-Tech Geopolitics Programme at the Takshashila Institution. His research interests are at the intersections of technology, geopolitics, and India's national interests, focusing on AI governance, open-source technologies, and telecommunications. He also manages the Graduate Certificate in Public Policy (Technology and Policy). Before joining Takshashila, he worked in telecommunications, developing software for 4G base stations.

Dr Brendan Walker-Munro is a Senior Lecturer (Law) with the Faculty of Business, Law & the Arts at Southern Cross University. Brendan's focus is on "research security" – the use of law and policy to protect university research from national security threats such as espionage, foreign interference, hacking, and unauthorised technology transfer. He also researches other aspects at the intersection of national security law and higher education, such as research funding, privacy, and digital security. Brendan is an Expert Associate (Adjunct) at the National Security College at Australian National University, Canberra as well as a Member of the Queensland Councillor Conduct Tribunal, the Disciplinary Panel of CPA Australia, and a Senior Research Fellow of the Social Cyber Institute.

Emeritus Professor Glenn Withers AO is a leading researcher in science and technology cost-benefit and regulation economics. He also researches population, skills and education, and culture, and is known for the development of the Australian immigration points system. He is a co-founder of the Crawford School of Public Policy at the Australian National University (ANU), Universities Australia and the Australia New Zealand School of Government. He has served as Head of the Economic Planning Advisory Council in Australia, President of the Academy of the Social Sciences in Australia and Board Chair of the Global Development Learning Network. He is a Board Member of Phenomics Australia, the Social Cyber Institute and the Social Cyber Group.

Inquiries

karthik@klude.in

greg.austin@socialcyber.co

https://www.socialcyber.co/social-cyber-institute/australia-india-tech-assessments