Technology Impact Assessment for Peace and Stability:

A Comparative Study on Australia and India

June 2025

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

Australia
India
Joint
Technology
Impact
Assessment
Project

Technology Impact Assessment for Peace and Stability:

A Comparative Study on Australia and India

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

June 2025

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

Project Overview

On 5 November, 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, ensuring 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 of Dr Jürgen Altmann, Professor Roger Clarke, Geetanjali Kamat, Pranay Kotasthane, Ujjwal Kumar, Dr Rajeswari Pillai Rajagopolan, Jayantika Rao Tiruvaloor Viavoori, Dr Ravi Srinivas and Dr Austin Wyatt. 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.

Executive Summary

Since 2020, Australia and India have committed to coordinating policy on critical technologies to promote peace and stability. This is part of a deepening political, economic and strategic relationship across many sectors. One of the policy tools for managing technology policy in both countries has been that of technology impact assessment (TIA), a process that has been in existence internationally for more than five decades. TIA is the systematic analysis of the impacts arising from the use of technologies. This includes both specialist assessment of their technical performance characteristics and cost-benefit considerations as well as consultations across diverse stakeholder groups (such as government, industry, academia, and society) to determine broader social, political, legal or economic consequences. In both Australia and India, there is only a modest record of impact assessments for critical emerging technologies affecting peace and stability. We could not easily identify cases of best practice by either country. This paper makes a case for greater use of such assessments and the adoption of more credible and more comprehensive evidence-based approaches. It has had to draw on global experience to arrive at lessons for Australia and India.

The peace and stability agenda of most countries is, in essence, the diplomatic face of national security policy – the practices of shaping, implementing or contesting international regimes or cooperative measures to enhance national security. This includes issues related to deterrence as well as common or cooperative security, such as conflict prevention, protection of global critical infrastructure, arms control, or plurilateral regimes for technology development. These issues may not lend themselves to the sort of expansive public consultation that most specialists have regarded as an essential element of modern TIA. Voters in Australia and India have not traditionally placed a high priority on the diplomacy of peace or cooperative security, where single technologies have been the main focus. In countries where TIA is most developed, its focus has been on domestic policy concerns such as health or the environment.

The global practice of TIA in support of peace and stability has emerged in various forms, with varying degrees of secrecy or transparency, and at different stages of technology development and deployment. Moreover, there are many distinctions between TIA focused on stability (e.g., as in the stability of cyberspace or shared space situational awareness) and those intended for the protection of peace (e.g., diplomatic aspects of deterrence or maintaining a geostrategic balance of technological power).

In addition, in the global practice of TIA, we see a tension between analyses that start with a technology-first approach and those that set out to address specific policy problems, with clearer implications for systemic risks and opportunities. The bias toward technology-first approaches has been aggravated by the increasing political attention paid to TIA as a tool of geopolitical competition between the US and its allies on the one hand, and China on the other hand, for leadership in R&D for dual-use technologies. The critical technologies agenda of Australia and, to a lesser extent in India's case, is more focused on variants of a "tech war" than on the positive contributions that new technologies might make to cooperative security, that is, the peace and stability agenda. This situation has arisen in large part due to escalating operations in cyberspace and the escalating confrontation between the US and China.

One of the notable recent examples of TIA of a class of technologies affecting peace and stability has been the US National Security Commission on Artificial Intelligence (NSCAI 2021). Over several years, this commission addressed issues of deterrence, peacetime technological competition with other countries, and the domestic foundations of US technological power. The Commission also analysed important military applications of AI, highlighting the grey areas and overlaps between a peace and stability agenda and issues of military power.

When we look at the practices of Australia and India, we find some excellent examples of TIA in support of peace and stability. We see this in the Australian planning for the prevention of nuclear accidents, which have become linked to the critical technologies agenda by the emerging influences of AI and cyber security

on long established nuclear safety processes. In India, the ongoing TIA for specific AI applications, such as facial recognition technologies, will likely have important policy implications for peace and stability. For the most part, TIA for peace and stability has not consistently been a high priority for either country. In TIA for peace and stability in Australia, parliamentary committees have been the leading actors while in India, security and technology agencies have been in the lead.

The broad framing we have observed from Australia and India on critical emerging technologies does not offer a clear direction as to methodologies for conducting TIA for specific technologies or their strategic impacts. Currently, there are no best practices for TIA, which explicates a defined approach and methodology articulated by scholars or officials. This ambiguity stems from the fact that TIA can be used for many different purposes while focusing on the concerns of different groups of stakeholders. Since 2022, a number of stakeholders (leading intergovernmental organisations, think tanks and specialists) have called for increased attention to TIA and more disciplined approaches, particularly emphasising effective stakeholder engagement, and consistently ethical, democratic and transparent processes.

It may not be useful to set rigid guidelines for how a country might undertake TIA with a focus on critical technologies for peace and stability. However, there are several benchmarks that we can use: an appropriate balance in focus between a very broad class of technology (such as AI) and specific sub-fields where the impacts are distinct from those of other sub-fields (facial recognition compared with chatbots); the scope and granularity of the technology being assessed; the depth and detail of specialist input; the recognition of the significant role of non-technical social, political, legal, and economic impacts; the breadth and depth of stakeholder input; the comprehensiveness of the analysis, which should include international and alternative perspectives; the timeliness of the assessment; and the relevance of the findings to diplomacy aimed at promoting peace and stability. An important cluster of non-technical specialisations that must be well represented in TIA for peace and stability includes international relations, international law, and strategic studies. There is also a need for clarity about the ethical frameworks to be applied.

Most countries now face choices about where in the machinery of governance the most effective forms of TIA for peace and stability can be seated: in the national parliament, in government agencies or statutory authorities, and/or in specially convened task forces or commissions of inquiry representing diverse specialists and stakeholders. The minimum requirement would appear to be a recognised institutional centre of gravity for TIA in each country and a set of basic principles.

Both Australia and India would benefit from a clearer commitment to regularised TIA of critical technologies for peace and stability. This would involve organisational reform and commitment of more resources, which could be justified by reinstating peace and stability to the policy status it enjoyed in the 1990s and the first decade of this century. A drift to more confrontational relationships in international affairs in the past decade should point to the need for more investment in TIA related to maintaining peace and stability, alongside the more readily accepted increases in investment in TIA for hard military capability or domestic security.

Table of Contents

List of Abbreviations/Acronyms

3G	Third generation wireless
4G	Fourth generation wireless
5G	Fifth generation wireless
6G	Sixth generation wireless
ABLE	Association of Biotechnology-Led Enterprises
AERB	Atomic Energy Regulatory Board
AI	Artificial intelligence
AICCTP	Australia India Cyber and Critical Technologies Partnership
ANAO	Australian National Audit Office
ANSTO	Australian Nuclear Science and Technology Organisation
ARDTC	Anti-Rogue Drone Technology Committee
ARPANSA	Australian Radiation Protection and Nuclear Safety Agency
ASIO	Australian Security Intelligence Organisation
ASPI	Australian Strategic Policy Institute
ASSOCHAM	Associated Chambers of Commerce and Industry of India
ATO	Australian Taxation Office
CAR	Civilian Aviation Requirements
CASA	Civil Aviation Safety Authority
CEA	Central Electricity Authority
CERT-In	Computer Emergency Response Team India
CET	Critical and emerging technologies
CII	Confederation of Indian Industries
CISAG	Computer and Information Security Advisory Group
CSIRO	Commonwealth Scientific and Industrial Research Organisation
CTPCO	Critical Technologies Policy Coordination Office
CUTS	Consumer Unity and Trust Society
DAE	Department of Atomic Energy
DARPA	Defence Advanced Research Projects Agency
DGCA	Directorate General of Civil Aviation
DISR	Department of Industry, Science, Energy and Resources
DOT	Department of Telecommunications
DRDO	Defence Research and Development Organization
DSTG	Defence Science and Technology Group
DTA	Digital Transformation Agency
EIA	Environmental impact assessment
eTA	Ethical technology assessment
ETG	Empowered Technology Group
FICCI	Federation of Indian Chambers of Commerce and Industry
FREE	Framework for Responsible and Ethical Enablement
IAEA	International Atomic Energy Agency
iCET	India Initiative on Critical and Emerging Technology
ICMR	Indian Council of Medical Research
IGIS	Inspector-General of Intelligence
IIS	Indian Institute of Science
IITs	Indian Institutes of Technology
IoT	Internet of Things
IPCC	Intergovernmental Panel on Climate Change
IPCC	International Panel on Climate Change

ISpA	Indian Space Association
ISRO	Indian Space Research Organisation
JCST	Joint Standing Committee on Treaties
JIC	Joint Intelligence Committee
MeitY	Ministry of Electronics and Information Technology
ML	Machine learning
MoCA	Ministry of Civil Aviation
NASSCOM	National Association of Software and Service Companies
NBN	National Broadband Network
NITI	National Institute for the Transformation of India
NNCTA	National Network for Critical Technology Assessment
NSA	National Security Advisor
NSAB	National Security Advisory Board
NSC	National Security Council
NSCAI	National Security Commission on Artificial Intelligence
NSCS	National Security Council Secretariat
NTSB	National Transportation Safety Board
ONI	Office of National Intelligence
PIA	Privacy impact assessment
PRC	Policy Research Cell
PSA	Principal Scientific Adviser
RBI	Reserve Bank of India
RPAS	Remotely-piloted aircraft system
SCSP	Special Competitive Studies Project
SIA	Social impact assessment
SPG	Strategic Policy Group
SPR	Satellite Centres for Policy Research
STI	Science, Technology and Innovation
TA	Technology assessment
TAG	Technology Advisory Group
TIA	Technology impact assessment
TIFAC	Technology Information, Forecasting and Assessment Council
TRAI	Telecom Regulatory Authority of India
TTDF	Telecom Technology Development Fund
UAS	Uncrewed aircraft system
UAV	Uncrewed aerial vehicle
UNCTAD	United Nations Conference on Trade and Development
UNDP	United Nations Development Program
UNODA	United Nations Office of Disarmament Affairs
USOF	Universal Services Obligation Fund
UTM	Unmanned Aircraft System Traffic Management

1. Introduction

Governments, businesses and communities around the world are becoming more concerned by how technological innovations affect their interests. To address such concerns, beginning around 2020, Australia and India set in train a stream of policy initiatives under the heading of "critical emerging technologies affecting peace and stability". An important but underutilised tool for the development of these policies is technology impact assessment (TIA). The practices, principles and methodologies for this stream of policy development are still evolving in both countries.

This discussion paper is the first of two in a project funded by the Australia India Cyber and Critical Technologies Partnership (AICCTP). The paper seeks to strengthen consensus among key stakeholders in the two countries by building a strong public case for more credible and comprehensive evidence-based approaches for TIA to address risks to peace and stability. The second discussion paper will address the diplomatic aspects relevant to the pursuit of joint TIAs by Australia and India. We are presenting this paper for discussion and review by stakeholders as part of our ambition to foster an international community of practice for technology assessment in support of peace and stability.

We would like to acknowledge the participation and contributions of a large number of specialists and stakeholders from the Indo-Pacific, Europe, Africa and the Americas.

The first section of this discussion paper addresses the definitional issues around critical and emerging technologies that impact the domain of peace and stability. In Section 2, an overview of the global practice of TIA is presented, as well as best practice for conducting TIAs. Section 3 documents the mechanisms for TIA in the context of peace and stability for Australia and India. And finally, Section 4 serves to document comparative case studies in Australia and India of critical technologies impact assessment focused on(1) nuclear accident prevention and management; (2) artificial intelligence; (3) aerial drones; and (4) 5G/6G wireless technology.

In addition to the list of references cited in the paper, we provide a short reference bibliography of additional recent works in Appendix 1. This project has involved consultations with a range of practitioners and specialists in the field and the provision of expertise from the nine project team members whose experience is noted in Appendix 2.

Our approach is rooted in ethical frameworks for technology assessment, developed in Sweden as early as 2005, and addressing such topics as: control, influence and power, impact on human values, international relations, and gender, minorities and justice (Palm and Hansson 2005). This project is steeped in the broader context of peace and stability, which also incorporates human security (Alkire 2013; Michael et al. 2025), as well as interstate security (Michael et al. 2023; Chmielewski 2024).

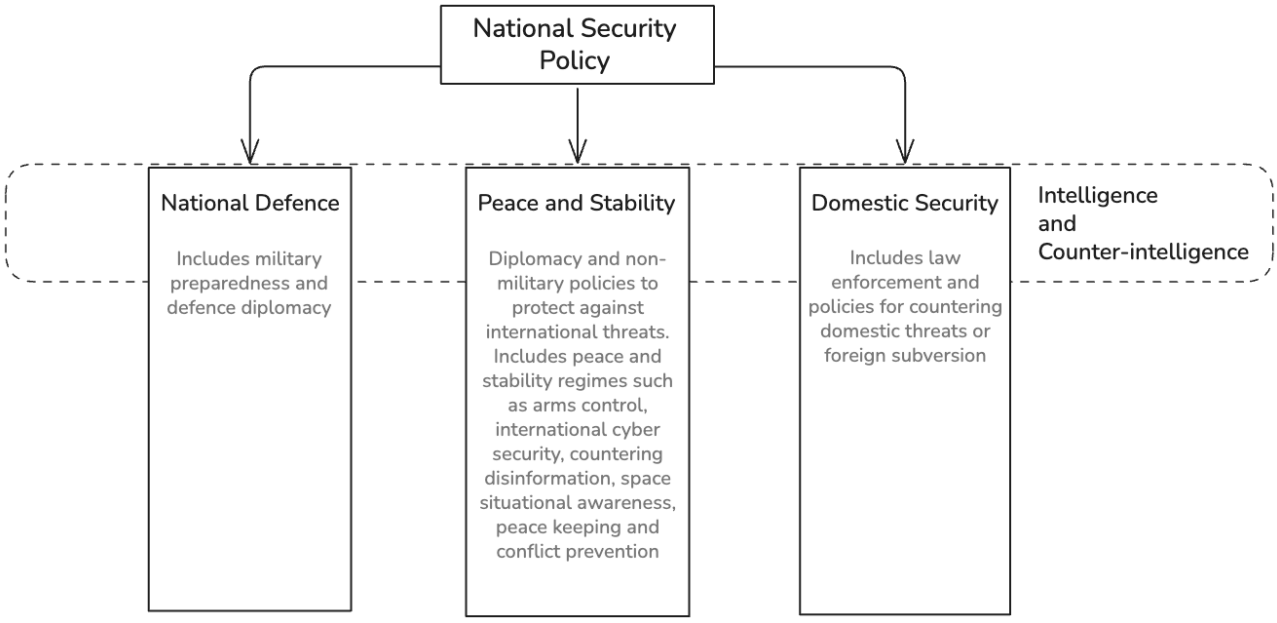
The approach presented in this paper for evaluating TIA is somewhat permissive and is not meant to be a universal rubric. Rather, the paper gives a perspective that should allow any stakeholder in a TIA to determine their level of confidence that a comprehensive specialist analysis has been or is being undertaken with a reasonable standard of coverage and objectivity, and with competing stakeholder interests and perspectives incorporated, based on reasonable and transparent opportunities for effective consultation.

1.1 Defining Peace and Stability

Peace and stability can be seen as one of three organising pillars in national security policy as illustrated in Figure 1. 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 technology controls. We exclude 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 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.

Figure 1: Pillars of National Security Policy



The three pillars of national security policy are far from equal in terms of priority and urgency. This is reflected in the relatively low priority attached to funding of TIA for peace and stability compared with TIA in the other pillars. More attention is paid to TIA for peace and stability issues only if they overlap with significant aspects of national defence or domestic security. This has been demonstrated recently by TIA in several countries with respect to artificial intelligence, as discussed in Section 4. In a similar vein, TIA impacting the intelligence function can often provide coverage of important peace and stability issues that might not otherwise receive attention.

1.2 Defining Critical and Emerging Technologies

In the case of Australia and India, the cooperation on critical and emerging technologies appears to extend beyond the normal scope of the concept of peace and stability to economic policy, social policy and public administration. The 2020 bilateral agreement on cooperation in critical technologies includes a long list of objectives and principles that address unambiguously core issues of peace and stability, alongside others that might be considered peripheral to the commonly held meaning of these words (India MEA 2020a):

1. open, free, safe and secure internet for citizens;
2. cyberspace as an economic enabler supporting the goal of prosperity and national development, especially through trade promotion;
3. countering cyber-crime or malicious state activity in cyberspace;
4. treating the increasing frequency of malicious state activities in cyberspace as having the potential to undermine national security and prosperity, and in turn, undermine international peace and stability;
5. protection of fundamental human rights and freedoms online;
6. opposing cyber-enabled theft of intellectual property;
7. ensuring that these technologies are used in a secure and ethical manner; and
8. cooperation in the protection of national critical information infrastructure.

At the same time, Australia and India also agreed to a Joint Plan of Action specifically targeting (1) the innovation economy (2) cyber security and (3) cyber-enabled critical and emerging technologies (India MEA 2020b). The last of these three sections concerned the economy, making specific mention of 5G, quantum computing, AI and machine learning. 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 controlling AI.

In the years since 2020, the focus of the two governments in their international policy on critical technologies has broadened and varies according to the forum of discussion. In Australia, the reference point became critical technologies of national interest, as captured in the 2023 policy *Critical Technologies Statement* (Australia DISR 2023). One view sees critical technologies as those that impact economic stability, national security, and social cohesion (Australian Trade and Investment Commission 2024, p. 47).

Australia has on occasion included the following technologies under the rubric of critical: (1) advanced manufacturing and materials technologies, including semiconductors (2) artificial intelligence (3) advanced information and communications technologies (such as 5G and 6G); (4) quantum technologies (5) blockchain (6) autonomous systems (7) robotics (8) positioning, timing and sensing (9) biotechnologies, such as synthetic biology (10) clean energy generation and storage technologies and (11) digital public goods, such as digital identity and digital payments systems (Australian Trade and Investment Commission (2024).

In a bilateral context with the US, and in a national security context, India has noted the following as critical: (1) space (2) semiconductors (3) advanced telecommunications (4) artificial intelligence (5) quantum (6) biotechnology and (7) clean energy (United States 2024). India, like Australia, also has referred to an equally broad set of ambitions: to ensure that technology is used in a manner consistent with "democratic values and respect for universal human rights" and "future security and prosperity" (United States 2024). India's vision is related to ensuring that technology is used in a manner consistent with further diversification of its military dependencies over the next few decades; strengthening lines of "strategic cooperation to deal with the challenge of economic overproduction in China; coproduce and co-innovate technologies to build geo-economic resilience; and potentially co-create new language in the complicated world of standards" (Chaudhuri and Bhandari 2024).

The Australian and Indian 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).

1.2.1 Emerging

The OECD has defined emerging technologies as those "characterised by rapid development and uncertainty in trajectory and impact" (OECD n.d.). These features present policymakers with the challenge of enabling innovation for economic and social benefit while simultaneously addressing "governance imperatives that anticipate risks, protect established rights and human agency". This perspective is supported by policy researchers. Rotolo et al. (2015) characterised emerging technologies as having the attributes of radical novelty, relatively fast growth, coherence, prominent impact, and uncertainty and ambiguity of use and risks. The classification of a technology as "emerging" is not a permanent label since "[a]s the technology matures, its novelty fades, and its uncertainty and ambiguity also reduce (Reddy and Naik 2025, p. 5).

For the purposes of TIA, an essential difference between a technology that is mature or established (e.g., nuclear fission) and one that is only emerging (e.g., quantum computing or 6G wireless) is the degree to which consequences are known, documented or proven. In the case of mature technologies, the tangible and intangible impacts are demonstrable, while in emerging technologies, the impacts are still being predicted, anticipated, or characterised. This distinction affects TIA in the degree to which foresight, estimation or assumptions need to be used in assessing likely social, political

or economic impacts. More assumption-based analysis is needed for emerging technologies than for mature technologies. Where mature technology is itself now changing as the result of rapid innovation (e.g., integration or convergence), the distinction between mature and emerging is quite blurred, implying a spectrum for the term rather than a precise or discrete categorisation.

While policy statements in Australia and India regularly refer to critical and emerging technologies, the candidate technology they refer to can be either established or emerging. There is also considerable ambiguity around the scope of "critical and emerging": do both characteristics need to be present, or just some combination thereof? Therefore, the term "critical and emerging" has not itself been adopted operationally for this paper; rather, we focus on the level of criticality in the context of an established or emerging technology, while understanding that the issue of pace of innovation can shape the degree of assumed or potential criticality.

1.2.2 Criticality

Schatzberg (2018) suggests that for a technology to be "critical" it must be the result of either: (1) a more involved elevated standard of science being applied, or (2) the technology's criticality, as a function of the importance that it accrues on its exposure to or diffusion in society. Bimber and Popper (1994) also approached the topic in this way, albeit from the lens of technologies that existed more than three decades ago. Their report defines four possible policy lenses for critical technology:

- As "high" or "advanced" technology, which "represents state-of-the-art, and is therefore the locus of innovation and an indicator of the industry's or nation's level of technical sophistication" (p. 15);
- As a component of State self-sufficiency, such that "technologies are deemed critical for ensuring security of the means for sustained economic growth and development – and in a complicated world economy, for 'competitiveness'" (p. 17);
- As a limitation or enabler for the delivery of some other beneficial outcomes, such as some manufacturing, service, or system capability which is in the interests of the State to acquire or develop (p. 20); and
- As a "generic and pre-competitive" quality, because early iterations of critical technologies are often multi-variate in use, where "development efforts are believed likely to produce a wide array of returns not tied to any specific product application" (p. 23).

These perspectives highlight the challenge of constructing a robust definition of critical technologies.

The first step in defining a critical technology is determining the precise level at which it is no longer "divisible" from similar technologies that constitute separate academic or industrial fields. As an example, one might consider the complex and nebulous field of quantum technologies, which incorporates fields across computing, cryptography, sensor design, atomic clocks, communication, simulation and metrology (Acin et al. 2018). Within each of these subfields are numerous other forms of technology. Continuing with the quantum computing example, it can be divided into quantum hardware, software, and applications from cryptography to large-scale computation (Gill et al. 2022). Advances in quantum technology in subfields, such as atomic clocks or magnetic resonance imaging (MRI), can be much more mature than other subfields, such as photonics.

The second step in determining an appropriate standard of criticality can be a determination of whether one technology or a subfield of it becomes critical when compared to another technology or sub-field, or by reference to its social, economic, legal, and/or geopolitical impacts. The emergence of the trade war in semiconductors between the United States and China after 2018 is an example of that last consideration (Fitch and Woo 2020; Miller 2022; Luo and van Assche 2023).

More recently, the Critical Technology Tracker created by the Australian Strategic Policy Institute (ASPI 2024) updated its earlier list of 44 key areas to 64 key areas. This Tracker adopts the Australian Government definition (Australia DISR 2023) that

critical technology is "current and emerging technologies with the capacity to significantly enhance, or pose risk to, a country's national interests, including a nation's economic prosperity, social cohesion, and national security." It includes a far wider selection of technologies such as metamaterials, distributed ledgers (i.e., blockchain), machine learning, directed energy, and electronic warfare to name a few. It is unlikely that even the wealthiest countries could afford to undertake in-depth TIA or even effective monitoring of 44 or 64 technologies from the point of view of their effect on peace and stability.

We take the view that a critical technology will have some mix of the following four characteristics:

- **Novelty.** This characteristic has two aspects. First, it can refer to technologies that have emerged within the last 5 to 10 years and are considered to be critical (Australia DISR 2023; ASPI 2024). Second, it can refer to mature or existing technologies that have new critical impacts as a result of changing geopolitical considerations or technical innovation (e.g., semiconductors).

- **Uncertainty**. A critical technology is often one where there is significant or substantial uncertainty about its potential implications for peace and stability, i.e., its military and/or dual-use possibilities at various levels of maturity or readiness.

- **Priority**. Critical technologies generally will have a strong connection to a national interest (Australia DFAT 2021). More often than not, critical technologies are linked to defence interests. How a State determines the boundary between defence interests and non-defence interests is outside the scope of this paper. However, the State does need to have a clear mechanism for determining when and where a given critical technology is in priority order; otherwise, the State risks proscribing or capturing every form of technology because it has an interest in what occurs within its sovereign territories. This is an extension of the well-known analogy that "if everything is national security, nothing is" (Dunlap 2021; Walker-Munro 2025).
- **Targetability.** This characteristic can otherwise be described as policy tractability. In order to be considered a critical technology, the hardware, software, product or process must be physically amenable to regulatory controls by a State (whether by law, policy or other means) to uphold its interests and control the diffusion and distillation of that technology. A technology that has already rapidly proliferated throughout society without regulatory containment is less likely to be classed as critical since the State no longer has a position of primacy over the diffusion of that technology.

From an Australian perspective, definitions of critical technologies have the force of law in some areas, replicating Ministerial and political interest in the subject (Brodtmann et al. 2023). For example, the same critical technologies defined by the lead agency, DISR, also appear in legislative instruments related to migration (Department of Home Affairs 2024). This means that Australian Ministers can regulate the entry of foreign nationals judged to be a net contributor or potential risk to national research in the target field. The same DISR technologies also appear in the Migration Regulations 1994 as amended in 2024 (Federal Register of Legislation 2024). These regulations enable cancellation of visas where "the Minister for Home Affairs is satisfied that there is an unreasonable risk of unwanted transfer of critical technology by the visa holder."

From India's perspective, it has neither a mandated list of critical technologies nor a strategy for the assessment and classification of them, though some evidence can be gleaned from recent bilateral and plurilateral partnerships on critical and emerging technologies. These include the US-India Initiative on Critical Emerging Technology, the India-EU Technology Trade Council, the UK-India Technology Security Initiative, and the Cyber and Cyber-Enabled Critical Technology Cooperation between India and Australia (Bachhawat et al. 2020). India certainly ascribes the critical descriptor to advanced telecommunications, space, quantum and artificial intelligence.

1.3 Selecting Critical Technologies that Impact Peace and Stability

In April 2021, Australia's formal policy, the "International Cyber and Critical Technology Engagement Strategy", identified three pillars: (1) values, (2) security, and (3) prosperity. The phrase "peace and stability" was used 17 times, in addition to "peace" being used 29 times and "stability" 21 times independently (Australia DFAT 2021). The strategy document also referred to "international peace and stability" (pp. 36-43) under the heading of "Security". Other headline elements of the security pillar were disinformation and misinformation, cybersecurity, cybercrime, online harms and safety. Within the pillar of "international peace and stability", the strategy committed Australia to "shape the development and use of critical technology, including cyberspace".

The core premise was that:

> "[t]he risks of malicious misuse of technologies can contribute to increasing strategic instability that, if unchecked, increases the risk of misperceptions and miscalculations between states that might escalate to conflict" (Australia DFAT 2021, p. 36).

The lines of policy action include:

- setting clear expectations for responsible state behaviour;
- deterring malicious activity enabled by critical technologies, including cyberspace, and responding when it is in the national interest;
- cooperating with other states to hold to account those who engage in unacceptable behaviour;
- implementing practical confidence-building measures to promote international peace and stability and prevent conflict.

Deterrence, arms control arrangements, and confidence-building measures sit firmly within the peace and stability section of the Strategy.

Otherwise, national defence and national security applications of critical technologies, including for the promotion of national defence industry, appeared in the Strategy's definitions to lie outside of the peace and stability section, for example under "strengthen national security", "protect our democracy and sovereignty", and "promote economic growth". But there is a grey zone, where the peace and stability interest would appear to overlap with interests relating to hard military application of critical technologies.

One of the most important aspects that underpins current Australian and Indian approaches to critical technologies is the concept of strategic technological competition. This is the concept that technology will contribute a greater proportion of national power in the future, and that getting ahead in some of these domains will give a disproportionate advantage that will only increase over time. This is tied up with the concept of 'tech war' along various fault lines of international security, most notably between the US and China. Australia has aligned with the US on a broad front, while India has supported the US in several discrete channels, most notably in supply chain considerations and in critical infrastructure investments.

2. Best Practice in TIA for Peace and Stability

Since 2022, there has been significant interest in the practice of TIA globally, among governments, international organisations, large commercial enterprises and scholars. A number of key players and researchers have called for more discipline in the process of TIA, as well as more effective stakeholder engagement, consistently ethical and democratic processes, or transparency. These include the National Network for Critical Technology Assessment in the United States (NNCTA 2023), the United Nations Conference on Trade and Development (UNCTAD 2024), RAND Australia (Dortmans et al. 2022), and the International Institute for Strategic Studies (Austin 2024). In June 2025, the Institute of Technology Assessment based in Austria convened an international conference over three days (ITA 2025). They billed the event as the "first Global TA conference". The seven-member Advisory Board for the conference included specialists from Australia (Peta Ashworth) and India (Krishna Ravi Srinivas).

TIA comes in many different forms and institutional settings, for a large variety of purposes. Table 1 provides a list of representative examples of publicly available TIA products by sector and level affected (i.e., national or international). Some products mentioned are final reports while others lay the foundations for a process of continuing deliberation. In this Section, we first consider key dimensions of TIA and then methodological aspects of TIA. We then examine how TIA processes can be shaped by supporting the goal of peace and stability.

Table 1: Examples of TIA by Sector and Level

Sector	Aspect of technology studied	Level affected	Related TIA product
Technology policy	Artificial intelligence development to maintain US supremacy (the declared aim)	National (US)	"The Final Report" (National Security Commission on Artificial Intelligence 2021)
Technology safety	Safety of ICT systems on 1 Jan 2000 (Y2K)	International	US legislation: "Year 2000 Information and Readiness Disclosure Act" (United States 1998)
Technology security	Foreign intelligence access to 5G telecommunications systems from China	National (UK) International	"Annual report of the Huawei Cyber Security Evaluation Centre (HCSEC)" (United Kingdom 2021)
Science and society	Human genome editing	National (US) International	"Human genome editing, science, ethics and governance". (National Academies 2017)
Aviation	Boeing 737 MAX flight control	International	"Boeing 737 MAX Return to Service Report Overview of the Technical Investigation Activities Performed by EASA" (European Union Aviation Safety Agency 2021)
Aviation	Drones	National (US) International	Sustained program of research papers and reports in the NASA series, "Advanced Air Mobility Mission" (United States NASA 2025)
Aviation	Carbon impact of fossil fuels	International	"Summary of fuels-related information from the ICAO Long-term Aspirational goal (LTAG) Analyses" (ICAO 2022)

2.1 Key Dimensions of TIA

The modern concept of TIA has been traced back to US Congressional discussions in 1966 in reviewing the impacts of supersonic flight. The concepts of environmental impact assessment (EIA) and social impact assessment (SIA) emerged at about the same time, with the former concept being legislated in the US in 1969.

In 1972, Congress passed the Technology Assessment Act to equip itself with "competent, unbiased information concerning the physical, biological, economic, social and political effects" of critical emerging technologies (United States 1972, p. 797). The roots of TIA in the parliament of a liberal democracy at the time, in this case the US Congress, reflected the necessary implication of considering social and community inputs, mediated by the parliament, rather than the executive branch of

government. Based on this history, there is a necessary implication that impacts (social, political, legal or economic) beyond technical performance must figure in all TIA.

The term TIA is often used interchangeably with "technology assessment", "technology evaluation", or even "technology testing". While "technology assessment" (TA) is more prevalent in the literature than "technology impact assessment", as Clarke (2025) notes, if "consequences" and "impacts" are treated as synonyms, technology assessment (TA) and technology impact assessment (TIA) are equivalent. Grunwald (2009) notes, "No consensual, unambiguous and selective definition of TA has yet been provided".

The TAMI (Technology Assessment Methods and Impact) project, involving several European Technology Assessment (TA) institutions, aimed to understand and improve the impact of TA on policy and society, addressing the definition of TA. Decker and Ladikas (2004) define TA as a "scientific, interactive and communicative process which aims to contribute to the formation of public and political opinion on societal aspects of science and technology". Banta (2009) offers a definition of TA as "a form of policy research that examines short- and long-term consequences (for example, societal, economic, ethical, legal) of the application of technology ... to provide policy makers with information on policy alternatives."

From these definitions, it is evident that even though TA may not reference impact in its label, it is usually not just about assessing the technology, a process largely dependent on technologists, but also about assessing its societal impact, which requires both a stakeholder-focused, participative approach and processes heavily reliant on social scientists. Even in the early days of TA in the 1970s, the emphasis was rarely exclusively on the narrow technology impacts, a fact that can be attested by reference to the list of OTA reports in 1974, 1975 and 1976 and hearings of the OTA Board on the non-governmental practices of TA in the US (United States Congress 1976).

TIA can be applied to a single application of a technology (e.g., driverless cars) or to a broader group of technologies (e.g., vehicle sensor systems). A similar comparison may be made between the distinct applications for AI-enabled facial recognition compared with the broader class of technologies in the many fields of AI.

The TIA process is commonly applied at the level of government regulation within countries, addressing the safety or efficacy of a technology, where the goal is to regulate the safety performance qualities of products, according to national standards. In many cases, TIA is conducted as a precursor to the formation of national standards. But TIA can also be applied at many other levels of social organisation across diverse sectors. For example, TIA has been used in the context of human and planetary security, as in the case of the Intergovernmental Panel on Climate Change (IPCC), the United Nations body for assessing the impacts of the continuing use of hydrocarbon fuels.

Just as TIAs can be undertaken on many levels, TIA is also a process that can be undertaken for various purposes. We favour an approach to TIA that takes as its departure point a policy problem, (such as threats to peace and stability from quantum sensing) rather than a technology-centric pathway (such as comparing quantum sensing technologies in the US and China). This means that our approach to TIA includes holistic analysis of systemic risks (e.g., the stability of cyberspace or supply-chain disruptions) and, importantly, opportunity and equity considerations (Clarke 2025; Naik et al. 2024). Often, there can be significant crossovers and perceived trade-offs between the purposes of a TIA as a product, and TIA as a process.

TIAs can take on a political and social life of their own. The assessments and processes have the capacity to affect the interests, rights and obligations of individuals, communities, businesses, governments, political parties and international entities Clarke (2025).

From an ethical point of view, there has been a growing realisation that technology is not neutral and is embedded with normative values that can significantly impact society. The ethical questions that arise from adopting technologies necessitate confronting the trade-offs affecting various stakeholders (Michael 2021). A technocratic approach with biases ingrained while building the technology may not always be the best suited for the task at

hand. A more participatory, stakeholder-focused approach is essential.

The process of TIA can be, at the outset, a highly politicised exercise engaging scientific or technical controversies, competitive business interests, and international relations. The breadth of the challenges in TIA, especially on the ethical front, can be seen in the identification of a 'legitimation trap' in all TIA (Weingart 1991, pp. 8-9). This is the idea that if a TIA has been done, that should be the end of any debate about the consequences of deploying the technology. The assumption is that TIA simply means asking the right specialists the right questions and then providing them the time and resources to research the questions, allowing for the estimation of technological impacts. This, of course, ignores the fundamental premise that all technologies have a lifecycle and physical lifetime, and context matters. These considerations underscore the need for ethical TIA, as advocated by Palm and Hansson (2006) and Kiran et al. (2015).

2.2 Methods of TIA

Technology assessments have been described as an early warning to policymakers on the risks or opportunities of the technology (Grunwald 2009). The classical or scientific approach to technology assessment is based on deep analysis regarding the technology and its sociological or economic implications. The goal is to provide objective information about a technology's impacts and alternatives for decision-makers. However, such approaches have their limitations in being able to anticipate impacts on diverse groups of stakeholders or in resolving ethical trade-offs between them (Grunwald 2009). This calls for more participatory methods of technology assessment. The practice of technology impact assessment has shifted from primarily expert-driven scientific approaches to include more participatory methods over time. This transition reflects broader societal, political, and methodological changes aimed at democratising decision-making (e.g., the role of participatory budgeting). Involving diverse stakeholders from government, industry, academia and civil society through transparent and open processes also builds legitimacy into the decision-making process. Some of the scientific and participatory approaches in TIA are described below.

2.2.1 Scientific approaches

Cost-Benefit Analysis: This is a structured analytical approach to assess whether the expected benefits of developing and deploying a certain technology outweigh the associated costs over a specific time horizon. The main goal is to estimate as many of a technology's positive or negative impacts as possible, in monetary terms, to aid decision-making. These include direct and indirect costs, tangible and intangible benefits and also opportunity costs. Indirect costs and intangible benefits include various aspects, such as environmental impact, health considerations, time savings, relationships, non-monetary benefits, and secondary market impacts. However, due to factors such as data accessibility and accuracy, the overall completeness of the analysis can be a challenge. Boardman et al. (2017) provides a systematic approach detailing various aspects of this analytical approach, positioning it as a powerful tool to aid decision-making rather than the sole determinant.

Systems Thinking: The technology decision-making environment is a complex, dynamic, and interconnected system. A holistic approach is required to understand how things influence and interact with each other within the whole system instead of focusing on individual parts in isolation (Ackoff 1994). Systems thinking involves modelling interactions between individual agents and systems to understand their behaviour, predict outcomes, and evaluate potential impacts. The approach has evolved as a separate discipline and has not been conventionally associated with technology impact assessment. However, it is a useful approach that helps to identify patterns, feedback loops and unintended consequences that can emerge from agents and systems optimising for various factors (Senge 1990).

Delphi method: This is a structured approach for gathering insights from a panel of experts. It is an iterative process that aims to elicit and refine opinions on a topic. It involves iterative rounds of questionnaires, with feedback being shared in between rounds. Participants remain anonymous during the process, preventing authority or personality from influencing the free expression of opinions. Dissenting views or rare opinions have a higher chance of being considered by the broader group in this process. Despite being a method that originated

over 50 years ago, the Delphi method is still a relevant tool for forecasting and decision-making based on expert opinion (Landeta 2006).

Bibliometric studies: These studies are research methods that use statistical and mathematical techniques to analyse bibliographic data. This data typically includes scholarly publications such as journal articles, books, conference proceedings and patents. Bibliometric studies can provide quantitative insights into research outputs, trends, patterns, and the impact of scientific and scholarly communication. They also provide insights into the geographic distribution of research, such as where research is concentrated or which countries are leading (Moral-Muñoz et al. 2020). In our view, bibliometric analyses are a good proxy measure of relative national capabilities in particular sectors because of the internationalisation of scientific activity. But they remain a proxy measure, meaning somewhat superficial and quick, rather than strong evidence that would require protracted multidisciplinary research by teams of specialists.

2.2.2 Participatory approaches

Scenario Planning: This strategic planning approach involves developing a set of plausible alternatives about how a future technology might unfold, rather than relying on a single forecast (Bradfield et al. 2005). It involves identifying key drivers of change, such as technological advancements, market trends, political considerations, economic considerations, societal shifts and geopolitical events. Scenario planning helps to identify opportunities and risks in multiple future states and plan strategies to adapt to the different scenarios. Involving diverse stakeholders in this process is essential for ensuring a comprehensive view and identifying potential blind spots.

Multi-stakeholder Impact Assessment: This involves deliberations between diverse stakeholders with the purpose of building consensus around potential impacts and proposed solutions. The nodal agency assessing or governing the technology must bring stakeholders from government, industry, academia and civil society to participate in conversation and consensus-building. The need for such mechanisms is more pronounced in a rapidly changing technology environment, as conventional governance mechanisms fail to keep up with the pace of technology advancement (Hagemann et al. 2018). Reddy and Naik (2025) propose a framework for identifying stakeholders across government, market, individual, and societal groups, highlighting their primary concerns and the tensions between them. Similarly, Clarke and Michael (2024) introduce a framework for multi-stakeholder risk assessment that involves conducting multiple parallel risk assessments from the viewpoints of various stakeholders and integrating these perspectives into a consolidated overview. Such multi-stakeholder impact assessment frameworks are underutilised in practice and have the potential to address significant gaps in current assessment practices.

Sandboxing: Regulatory sandboxes help to create an environment that facilitates the development, testing and validation of technology in a controlled environment before deployment in real-world scenarios. This approach aims to improve compliance, share best practices, contribute to regulatory learning, and foster innovation. The World Bank has developed a guide for policymakers and regulators covering key considerations for designing and implementing a sandbox (Jeník and Duff 2020). The Reserve Bank of India has implemented regulatory sandboxes in fintech that can prove useful in providing feedback for evidence-based policy, although they might not replace other multi-stakeholder mechanisms such as consultations (Shashidhar 2023).

2.3 TIA for Peace and Stability

In general terms, the practice of TIA for peace and stability has emerged in a large variety of types or formats, with varying degrees of secrecy or transparency, at various stages in the development and maturation of a target technology, for various durations, or including a single stakeholder or several. Moreover, there are many distinctions between TIA undertaken with respect to concepts of stability (as in the stability of cyberspace or stability of a technological balance of power), and TIA undertaken in support of peace (reducing war risks and/or uncertainty through analyses related to the dictates of deterrence or a geostrategic balance of technological power).

One of the most notable examples of TIA for peace and stability has been the US National Security Commission on Artificial Intelligence (NSCAI 2021), which over several years addressed issues of deterrence and warfighting, alongside peacetime technological political competition with great power rivals, and foundational US technological power. Set up in 2018 by the US Congress, it was co-chaired by Eric Schmidt (former CEO of Alphabet) and Robert Work (former Deputy Secretary of Defence) and included 15 Congressional appointees, representing technical specialists, business executives, academic leaders, and international security professionals.

The commission championed transparency in its operations, holding five public plenary sessions over 15 hours of deliberations that were streamed live online and archived on the NSCAI website. The commission responded to over two dozen Freedom of Information Act requests and released more than 2,500 pages of material. Additionally, it posted over 700 pages of draft materials for public review and comment. With a view to building consensus on recommendations, the Commission engaged with a wide range of stakeholders, including civil society, private sector, government groups, ethicists, technologists, national security strategists, warriors, diplomats, academics, and entrepreneurs.

Of note, a critique of the Commission published one month after the release of the Final Report identified several shortcomings. The author observed the dominance of the military superiority ambitions of the US, the fact that it is in an "inescapable arms race with China", and that autonomous weapon systems developed "in the interests of the United States" are inevitable (Suchman 2021). The author observed that "[t]here is no space devoted to considering alternatives to the expansion of a national security strategy based on US military and technological dominance—for example, through greater investment in humanitarian aid and international diplomacy". She called on Congress and the US President's Office of Science and Technology Policy to critically review the Commission's recommendations and subject them to debate "in a forum that opens the discussion to a broader range of expertise and visions for greater security".

In the same year the report was published, the chair of the Commission, Eric Schmidt, set up a new bipartisan, non-profit organisation to continue the Commission's work, the Special Competitive Studies Project (SCSP). The focus was to expand the focus of public policy beyond national security to support for the US in winning the 'techno-economic competition' (https://www.scsp.ai/). This is one area where the notion of dual-use technologies is highly relevant to any TIA-related discussions.

We can identify several important dimensions that have featured in TIA work related to peace and stability or national security, broadly defined, in the past decade.

2.3.1 Geopolitical Considerations

Narratives around technology sovereignty, supply chain security and technostrategic autonomy have become more prominent. Policy efforts are focused on removing bottlenecks, outpacing rivals, or even denying access to crucial building blocks for the technology. For instance, the recently announced AI Diffusion Framework (Heim 2025) and America First Investment Policy (United States 2025b) are examples of some such initiatives that aim to sustain and enhance the global AI dominance of the US.

Drezner (2024) argues that post 9/11, the scope of national security has continuously expanded to include everything from climate change to artificial intelligence to critical minerals. With this expanding scope, Drezner points out that political and market incentives exist to label something as having national security implications, and bureaucratic incentives work against downgrading it. When everything is considered strategic, nothing can be prioritised. A more discretionary approach to what is strategic or critical may be required. This discussion paper attempts to articulate the approaches towards critical emerging technologies and peace and stability in Australian and Indian policy contexts. But these definitions have a very broad ambit, and further refinement is required.

2.3.2 Technology maturity

Technological progress typically follows an S-curve, moving through the stages of scientific discovery, invention, commercialisation, adoption and commoditisation. During the early stages of discovery and invention, an understanding of the opportunities and risks of the technology is still evolving. As technology becomes commercialised and adoption increases, the understanding of its impact improves; however, the scale of that impact is also greater. NASA's technology readiness levels (Mankins 2009) are a type of measurement system used to assess the maturity level of a particular technology. While the system was developed for the assessment of space technologies, the classification is applicable and useful for discussing technology development stages and helps guide decision-making in other technologies as well.

However, when it comes to technologies that have diffused across various segments of society, the TIA should not be limited to a linear dimension of technology maturity but should also include additional dimensions of technology diffusion and temporal evolution of its impact. The impact assessment of a technology could be different when its usage is higher than when it is lower. Similarly, as technologies become more embedded within societal structures and practices, their consequences often unfold gradually. Therefore, effective TIA must be longitudinal, even after the technology has reached maturity. This approach enables a more nuanced understanding of both immediate and latent effects, ensuring that assessments remain responsive to the shifting relationship between technology and society.

For instance, the widespread adoption of semiconductors has led to the emergence of implications that were not evident in earlier stages, even amongst trailing-edge chips. This illustrates that the scale and context of usage can generate new and unforeseen consequences. Similarly, the societal impact of social media usage among children only became apparent over time, as prolonged exposure revealed behavioural, psychological, and developmental effects. These examples underscore the importance of adopting a longitudinal perspective in Technology Impact Assessment, recognising that certain impacts may surface only after extended periods of interaction with the technology.

2.3.3 Comparison with existing technologies

When a technology is being assessed, it is helpful to compare its impact to its selection environment, i.e., alternatives or what it replaces. This includes practical considerations such as cost-effectiveness, increase in capabilities, long-term potential and environmental impact. However, the subtler effects of the impact on norms and behaviour are equally important, as new technologies could have a disruptive impact on them. As Postman (1993) posited in his book *Technopoly*, "Technology is not just additive; it is ecological", it can fundamentally alter the environment and everything in it. For instance, social media has changed not only how we connect with each other but also introduced challenges like mental health issues, political polarisation, misinformation, cybercrimes, a digital divide, privacy concerns and altered societal norms and behaviours.

2.3.4 Social and environmental impact

The adoption of new technologies may have significant effects on society and the environment. Its adoption might lead to winners and losers, with some groups benefiting from increased productivity and opportunities, whereas others might face reduced opportunities or job displacement. It might also exacerbate inequalities along existing fault lines, such as socio-economic, gender, or digital divides.

Beyond economic impacts, technologies also influence social, behavioural or cultural norms in ways that are not always obvious. This is clearly demonstrated by social media's impact on society and politics. Similarly, the environmental impact is equally significant. Technology adoption might require raw materials, energy, water and other resources and might generate pollution during its lifecycle. The ecological footprint might disrupt ecosystems and threaten biodiversity. Understanding both the negative and positive impacts of technology is essential for responsible adoption.

The broad framings we have seen from Australia and India on critical technologies do not grant a clear direction as to methodologies for conducting TIA of particular individual technologies or of their strategic impacts operating in combination with other factors. Key statements involving Australia and India on critical technologies, such as the bilateral statement (India MEA 2020a) and the Quad statement from the White House (United States 2021), do not provide any guidance on the sort of TIA that might be used for capabilities affecting peace and stability. The bilateral statement appears to consider security interests that are confined to a "stable and secure cyberspace". The United States (2021) refers in broad terms to "fostering an open, accessible and secure technology ecosystem, based on mutual trust and confidence". This approach emphasises transparency and trust as the main criteria for TIA with respect to critical technologies, rather than focusing on definitions of peace and stability.

Neither Australia nor India has the resources to undertake such an assessment for every one of the technologies they have identified as critical technologies. This is an even more important consideration when we consider the numerous and diverse subfields of new areas, such as quantum sensing (Austin 2024).

Moreover, some TIAs typically have more limited purposes than others. Some are intended to shape national defence industry priorities or choices about national subsidies, such as choosing between high funding levels for quantum sensing or artificial intelligence. Other TIAs have more expansive purposes that include assessments of the impact of inter-state deterrence on a set of intelligence-related technologies (space ISR, command and control, combat analysis) that affect decision advantage in wartime or crisis. This latter case would involve the ecosystem impacts of diverse technologies as applied in military posture and readiness levels, and not simply assumed advantages of one country in a number of unintegrated and separate technologies. Converging technologies at every level- systems, networks, services, applications, data play a significant role in determining technology impact assessment in a holistic manner, not piecemeal.

At the outset of the project, the most credible approaches to TIA for a candidate technology affecting peace and stability are: (1) those that are more comprehensive, assessing multi-sector inputs, outputs and outcomes; and (2) those that are more granular assessing sub-fields and applied technologies rather than the basic science of broad categories, such as quantum sensing or artificial intelligence.

2.4 Foundational Benchmarks

We conclude that it is probably not useful to set rigid guidelines for how a country might undertake TIA affecting peace and stability. However, we can identify several aspects of how the terms of reference for a TIA might be constructed for the most effective outcomes. We can identify benchmarks for TIA around a range of metrics:

- 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;
- recognition of the central place of the social, political, legal, and economic impacts;
- comprehensiveness of analysis, including international and alternative views;
- timeliness;
- high relevance to policy for peace and stability;
- a clear ethical framework.

Then, depending on how well a specific TIA approach achieves those benchmarks, we can assess its quality as advanced, intermediate or basic. An advanced TIA would meet all these benchmarks quite convincingly. A basic TIA would meet only a few.

3. Mechanisms for TIA in Australia and India

Australia and India have had quite different approaches to TIA for peace and stability, as a result of divergent priorities in domestic government policy, development models, the character of their innovation systems, governance systems and strategic policy.

3.1 Australia

Australia's recent practice of TIA has concentrated on health and agriculture, but this work has included some national security aspects. Some of this work is reflected in the Horizon-Scanning series of reports on technology conducted by the Australian Council of Learned Academies, a peak body for scholarly fellowship. Conducted over the period 2017-2022, this series began with agricultural technology and energy but then moved into precision medicine and synthetic biology and across to AI and the internet of things. The Horizon Scanning series was commissioned by Australia's Chief Scientist (ACOLA 2017, 2018, 2019, 2020). ACOLA continues to work on technology futures and impacts in seminars, conferences and individual reports.

Australia has a network of institutions and diverse formal processes for impact assessment of critical technologies through the lens of peace and stability. These assessments have informed decisions that range from AI governance frameworks, counter-terrorism policy, setting development priorities for the intelligence community, cybersecurity, arms control, and infrastructure bans for foreign equipment (e.g., broadband network and 5G wireless).

Table 2 below provides a list of TIA examples from Australia, along with the associated actors, the technology under assessment and the main concern the TIA is addressing.

Table 2: Illustrative List of Australian Technology Assessments Relevant to Peace and Stability

Technology	Actors	Main concern	Product
AI	Parliament Government Industry Community	National security	"Select Committee on Adopting Artificial Intelligence: Final Report" (Australia Senate 2024a)
AI	Government agencies, Research specialists	Peace and Stability	"Australia's Submission to the United Nations Secretary-General's Report on Lethal Autonomous Weapons Systems" (Australia 2024)
Telecoms security (5G)	Government Parliament Industry Community Allies	National security	"Review of the Telecommunications and Other Legislation Amendment Bill 2016" (Australia Parliament 2017)
Quantum	CSIRO (Government Research)	National security	"Growing Australia's Quantum Technology Industry" (Australia CSIRO 2020)
Advanced technology	Intelligence Research specialists	National security	"Social Science Research and Intelligence in Australia" (Withers et al 2019)
Data economics	National (Australia)	Digital economy and security	"Australia's data and digital dividend Inquiry report" (Australia Productivity Commission 2023)

As the list suggests, TIA conducted by the parliament, non-executive agencies of the government, and non-government bodies are more accessible. There are certainly many undertaken by the government that are never mentioned in public or receive only scant attention.

One benchmark for the ideal situation was laid down by the Science Minister, Barry Jones, who took office in 1983 as part of the Labour Party Government. He said his Party had committed to setting up a new Office of Technology Assessment:

> "Technological sovereignty then, is the first step in minimising unfortunate side effects of technologies. Our platform set out others, notably public information and the establishment of two assessment and information bodies - an Office of Technology Assessment and a Commission for the Future. Information, open discussion and control of technological destiny are the essential elements in ensuring a future in which technological change occurs in a way which is both acceptable to the individual and beneficial to the community as a whole" (Jones 1983).

While successive governments over four decades have not set up an office of technology assessment, there are many reasons why Jones' argument holds true today and is even more pertinent. That said, what matters most may be that governments commit to certain standards, rather than the precise format of a government agency assigned task. Jones emphasised the primacy of people-centred technology assessment, both at the individual and community levels.

In Australia, the practice of TIA for critical emerging technologies affecting peace and stability is underdeveloped. This has been illustrated very well by a RAND report commissioned by the Defence Science and Technology Group (DSTG) (Dortmans et al. 2023). The task was to "develop an analytical framework to support the prioritisation of [Critical Technologies of National Interest] CTNI" (Dortmans et al. 2023, p. ix). There was a blend of national security issues with those of industry development, but with a focus on an international crisis, in the event that Australia might not be able to count on the regular supply of these technologies that prevails under normal conditions.

Despite the report not using the language of peace and stability, it certainly addressed the terrain. The report noted the Australian government's definition of CTNI as "current and emerging technologies with the capacity to significantly enhance, or pose risk to, our national interests (economic prosperity, social cohesion and/or national security)" (Australia, CPTCPO 2021, p.1). The report correctly identified tensions between the country's needs in these three different domains. It said that "The competing policy objectives of security, prosperity and social cohesion suggest the need for a technology assessment for CTNI that is distinct from (but related to) parallel efforts in the Department of Defence, which primarily focuses on security" (Dortmans et al. 2023, p. xii). It identified a broad range of factors outside of technical considerations that should be influential in technology assessment, given their interdependence with technical aspects. These included infrastructure, workforce, supply chains and international competition. The report argued for a consistent, transparent and functional decision framework that can be optimised to the circumstances of the day.

The report advised the government to adopt a flexible methodological approach to assessing technologies for their relevance to the CTNI criteria:

> "given that the nature of the policy environment is highly interdependent and both context- and time-dependent. There is no single optimal solution. Rather the result will be a 'best fit', given the circumstances of the day and the shifting perspectives of those making the assessments" (Dortmans et al. 2023, p. xii).

TIA mechanisms in Australia have included national security reviews, commissioned reports, standard-setting initiatives, and public inquiries. Unlike the US, where many public inquiries have addressed technology competition at a geopolitical level, Australian TIAs that have been published with open access have more often taken a domestic national security (stability) angle. Where the Australian investigations have crossed into geopolitical issues, these efforts have emulated those of

the US in attempting to counter authoritarian agendas.

Australia did set up the Critical Technologies Policy Coordination Office (CTPCO) in the Department of Prime Minister and Cabinet (PM&C) to provide coordinated, whole-of-government advice on technology developments, opportunities and risks, and to recommend actions to promote and protect the development and deployment of critical technologies. The Unit was subsequently assigned to the Department of Industry, Science and Resources and in our view lost something of the whole-of-government perspective in favour of more narrow focus on economic and industrial policy.

The primary actors in Australian TIA can be listed as follows, while recognising that for any single TIA, there will be a variety of combinations, interacting through formal and informal relationships:

- Committees of the national parliament
- Intelligence agencies (ASD, ASIO, DIO)
- Executive departments (Defence, Foreign Affairs, Industry)
- Non-executive agencies (DSTG, CSIRO)
- Specialist groups (National Academies, universities, think tanks)
- Industry groups
- Non-governmental organisations (Electronic Frontiers Australia).

3.1.1 Committees of the National Parliament

Reports by committees of the Australian parliament come closest to consistent best practice in TIA of critical technologies for peace and stability, in terms of criteria such as comprehensiveness, specialist depth, stakeholder consultation, and transparency.

The best example is from 1989, when the Senate Committee on Foreign Affairs, Defence and Trade published its report on *Visits to Australia by nuclear-powered or armed vessels: Contingency planning for the accidental release of ionising radiation* (Australia Senate 1989). The report, over 670 pages, was unprecedented in Australian parliamentary history for its technical depth, political breadth and considerate treatment of radical views. It has not been surpassed in these respects. Moreover, that inquiry has not been surpassed by any in Australia for the seriousness and gravity of the immediate risks to peace and stability posed by public attitudes to critical technologies. For more information on the nuclear warships inquiry, see Section 4 of this paper on case studies.

The role of the parliamentary committees in critical technologies affecting peace and security subsided until the beginning of the war on terror after 2001 and then accelerated again after 2011 when political relations between Australia and China, and later Australia and Russia, began to break down. Interest further accelerated as US President Trump initiated the technology war with China beginning in 2018.

Almost all of these reports addressed general policy settings for critical technologies as a group, rather than an investigation into granular technical detail or sub-fields. For example, the Senate Select Committee on Adopting Artificial Intelligence tabled its report in December 2024. The inquiry was conducted in less than one year with 245 public submissions, and 72 witnesses. Wide coverage of economic, business and social impacts, as well as some national security issues. There were only seven references to the term “national security” and none to “peace” or “stability”. There is little analysis of the details of how any aspect of AI specifically impacts national security issues. In another 2024 report, “Supporting Sovereign Capability in the Australian Tech Sector”, by the Senate Finance and Public Administration Reference Committee, there was almost no technology assessment to speak of (Australia Senate 2024c).

Many parliamentary inquiries canvassed critical technology issues as a very small part of a bigger economic policy agenda. This can be seen in the government’s response to a committee report on shutdown of the 3G mobile network (Australia Senate 2024d). Passing references to technology impacts on privacy have featured in parliamentary bills amending telecommunications legislation to counter terrorist threats. In spite of its leading position in Australia as the best single source of technology assessments available to the public and involving many stakeholders, the parliament remains

somewhat timid in this area. For example, in its inquiry into the use of 5G in Australia, the House of Representatives Standing Committee on Communications and the Arts (Australia House of Representatives 2020, p. vii) operated under a terms of reference that deemed matters relating to national security to be "out of scope for this Committee".

The Defence Intelligence Organisation (DIO) is the primary source for assessment of foreign technologies affecting kinetic war-fighting, while the Australian Signals Directorate (ASD) leads on assessment of technologies affecting cyberspace. In 2022, Australia established the Cyber and Critical Technology Intelligence Centre, a multi-agency initiative within the Office of National Intelligence announced in March 2022 (Australia ONI n.d.). This centre aims to produce novel cyber and technology insights to inform complex government decision-making and harnesses cyber and technology expertise to produce all-source intelligence assessments. The establishment of this dedicated intelligence centre reflects Australia's assessment that technological developments require specialised monitoring and analysis for national security implications.

3.1.2 Executive departments

The Defence Department, primarily through ASD and its DSTG, has the primary responsibility for assessing future impacts of most technologies through a function described as "technology foresight". DSTG assesses emerging and disruptive technologies, prioritising military readiness and asymmetric capabilities under the Defence innovation, science and technology strategy (Australia DSTG 2024). In 2022, DSTG also established a function called "Socio-Technical Futures Analysis" to assess the societal implications of emerging and potentially disruptive technologies (Australia DSTG 2022). The focal points of its modest funding announced in 2022 were to be as listed below (rendered verbatim), but there has been negligible public reporting under this functional descriptor since 2022:

1. concepts and theories that integrate or otherwise account for the interplay between emerging and potentially disruptive technologies and society;
2. comparative analysis of the consideration of social factors in international approaches to critical technology foresight;
3. analytical models for assessing the societal impact of emerging and potentially disruptive technologies;
4. methodologies for designing, developing and deploying technologies in a socially-responsible manner;
5. social analysis of technological convergence; and
6. the role of technology in preserving social cohesion in times of insecurity.

While it is difficult to find post-2022 activities by DSTG under this exact descriptor, DSTG continues to conduct horizon scanning and futures analysis in activities the banners of Emerging Futures and Emerging Disruptive Technology Assessment Symposium (EDTAS). These symposia involve DSTG partnering with universities and industry to deliver workshops and various keynote presentations. These annual events, which have the aim of future-proofing Australian Defence, could be seen as TIA of a kind but it is difficult to evaluate their lasting influence.

The Department of Industry, Science, Energy and Resources (DISR) leads the development and maintenance of Australia's "List of Critical Technologies in the National Interest". DISR coordinates public consultations, defines priority fields (e.g., AI, quantum, and advanced manufacturing), and aligns the list with strategic goals like economic growth, supply chain resilience, and sovereign capability. The agency revised the list in 2023 to focus on seven high-impact technology fields, informed by academic and industry input, while collaborating with security entities like the Defence Science and Technology Group. DISR also integrates the list into broader initiatives such as the National Reconstruction Fund to drive investment in critical tech sectors. DISR manages standards development, including through international standard-setting bodies. But it is difficult to discern exemplars of advanced TIA as outlined in Section 2 of this paper.

3.2 India

The priorities for technology assessment in India have evolved significantly since the country gained independence. Beginning in the 1970s, the move toward institutionalisation of TIA concentrated more on the health and environment sectors than on broader international integration and it was largely practised as an intra-governmental process (Jha-Thakur and Khosrav 2021). TIA became mandatory in 1994 for new nuclear energy projects. In 2017, The Department of Health Research (DHR) under the Ministry of Health and Family Welfare initiated a pilot program on Health Technology Assessment in April 2017, which led to the formal approval and establishment of the Office of Health Technology Assessment (HTAIn 2025).

India has embraced technology adoption, recognising its potential for socioeconomic uplift of its citizens. However, historically, there has been caution and scepticism surrounding the adoption of technology. In his book, *Midnight's Machines*, Arun Sukumar (2019) highlights that Jawaharlal Nehru, India's first Prime Minister, was hesitant to introduce everyday technologies that could directly enhance the lives of ordinary people, fearing that they might overwhelm or disadvantage marginalised communities.

Additionally, India's access to technologies necessary for nation-building and national security has been influenced by international relations and political circumstances. For instance, during the Cold War, export controls limited access to Western technologies because of India's non-aligned stance and its ideological proximity to the USSR. Furthermore, India's tightly-controlled and centralised economy before the liberalisation reforms of the 1990s, also hindered technology adoption.

In this environment, the practice of TIA in India, especially regarding issues that pertain to peace and stability, has often lacked broad public deliberation and dissemination. With India currently pursuing ambitious national programmes such as the IndiaAI Mission, National Quantum Mission, and National Mission on Interdisciplinary Cyber-Physical Systems, alongside pushing for rapid adoption of Digital Public Infrastructure, the need for robust TIA mechanisms to guide informed policy and decision-making has increased dramatically over the past decade. The dual-use nature of emerging technologies and geopolitical tensions surrounding their diffusion also make TIA indispensable as a tool for stability maintenance.

Table 3 below provides a list of TIA examples in the Indian context.

Table 3: Illustrative List of Indian TIA affecting Peace and Stability

Technology	Actors	Main concern	Key Product
Quantum	NITI Data Security Council of India	National security	"Quantum Computing: National Security Implications & Strategic Preparedness" (India NITI AAYOG 2025)
AI	MeitY Office of PSA Inter-ministerial Advisory Group Subcommittee (from government, academia, industry and think-tanks)	Technology governance Trustworthiness and accountability of AI systems	AI Governance Guidelines Report: Recommendations of the Sub-Committee on AI Governance and Guidelines Development (IndiaAI 2025)
Quantum	DST PMSTIAC	Capacity building	National Quantum Mission (India 2024a)
Outer space	ISRO	Safety Security Sustainability	"Indian Space Situational Assessment Report 2023" (India 2024b)
IT	RBI	Cybersecurity	"Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices" (India RBI 2023)

India adopts a more distributed approach to TIA compared to some countries that have dedicated parliamentary bodies for this purpose. TIA functions are typically conducted by various executive departments, such as line ministries, government advisory bodies and sectoral regulators. These organisations usually conduct broad consultations with stakeholders, including academia, industry organisations and think tanks, even though the private sector often expresses dissatisfaction with the intensity of these engagements, citing a lack of consistency and depth.

Whilst many line ministries conduct formal and informal TIA, the key agencies that oversee different aspects of governance of critical technologies affecting peace and stability are the National Security Council, the Department of Science and Technology (DST), Ministry of Electronics and Information Technology (MeitY), Department of Space, Department of Telecommunications and the Ministry of External Affairs.

For matters pertaining to defence and national security, the National Security Council (NSC), operating under the Prime Minister's Office, assumes the coordinating responsibility for TIA, reflecting the sensitivity assigned to this sector. The Defence Research and Development Organisation (DRDO), which is under the Ministry of Defence, also works on emerging technologies.

As a nodal agency responsible for orchestrating long-term national security planning and fostering inter-agency coordination on critical security matters, the NSC operates as a key advisory body. It is headed by the Prime Minister, supported by the National Security Council Secretariat, and includes various wings to address diverse security challenges:

- National Security Advisor (NSA): The NSA is the Prime Minister's principal advisor on security and strategic matters and oversees the functioning of the NSC.
- Strategic Policy Group (SPG): With NSA as the Chairperson, the SPG comprises the Cabinet Secretary, Secretaries of Defence, Home, External Affairs and Finance departments, heads of military, intelligence services and key scientific establishments and NITI Aayog. The SPG is the apex decision making organ of the NSC.
- National Security Advisory Board (NSAB): Comprising a panel of domain experts from diverse fields both within and outside the government, the NSAB provides independent analysis and strategic recommendations on national security issues.
- Joint Intelligence Committee (JIC): JIC coordinates intelligence inputs from Research and Analysis Wing, Intelligence Bureau and military intelligence agencies.
- The NSC is also the nodal agency from India for the Quad Critical and Emerging Technologies (CET) Working Group.

DST is the nodal department for formulating science and technology policies, promoting scientific research and development, and supporting indigenous technology development. It has a mandate to work with various stakeholders to study emerging technologies and provide policy advice. It currently supports several mission-mode programmes, such as those on cyber-physical systems and quantum. The department established the Policy Research Cell (PRC) programme in 2013 with the aim of providing public policy support for strengthening the Science, Technology and Innovation (STI) ecosystem in India. The programme operates through the establishment of DST Centres for Policy Research (DST-CPR), DST Satellite Centres for Policy Research (SPR) and the DST STI Policy Fellowship Programme.

MeitY is responsible for formulating regulations related to digital technologies, cybersecurity, artificial intelligence and data protection. Its initiatives are mainly related to national economic development of critical technologies (Digital India programme, IndiaAI Mission, and Indian Semiconductor Mission).

The Department of Space, working primarily through the Indian Space Research Organisation (ISRO), has oversight of R&D in the sector. It has established several expert committees and working groups comprising scientists and engineers

from within the organisation, government research organisations like DRDO, and academic institutes for technology evaluation and mission-mode projects like the Mars Orbiter Mission. It established the Indian National Space Promotion and Authorisation Centre (IN-SPACe) in 2020 to act as a nodal agency to facilitate private sector participation in the space domain.

The Department of Telecommunications (DOT) addresses the impact of emerging technologies like 5G, 6G, AI, and IoT mainly from the industrial development point of view. The Telecom Technology Development Fund (TTDF), set up under the Universal Services Obligation Fund (USOF) of the DOT, promotes research in emerging technology domains.

The Ministry of External Affairs established the New, Emerging and Strategic Technologies (NEST) Division in 2020 to coordinate India's engagement in global technology discourse.

Sectoral regulators in India conduct domain-specific TIA. While the general focus of such TIA is assessing the impact on market stability, consumer protection, competition, and overall sectoral development, they also encompass aspects related to peace and stability. Other regulators with a stake in critical technologies for peace and stability include the Reserve Bank of India (RBI), the Atomic Energy Regulatory Board (AERB), and the Directorate General of Civil Aviation (DGCA), for regulating the civil aviation sector.

Several government agencies outside of the executive branch play coordinating and advisory roles across various technology initiatives.

The National Institution for Transforming India (NITI Aayog) is India's premier policy think tank. It shapes policy direction for technology governance. Its initiatives include the NITI AAYOG Frontier Tech Hub (NITI-FTH) to foster engagement with experts across industry, academia and the government to assess the impact of emerging technologies, and the Science and Technology Division to strengthen India's STI ecosystem.

The Office of the Principal Scientific Adviser (PSA) serves as the chief authority for providing pragmatic and objective advice to the Prime Minister and the Cabinet on matters related to STI. It is supported by the Prime Minister's Science, Technology, and Innovation Advisory Council (PM-STIAC). This council is chaired by the PSA and comprises eminent experts across diverse domains from both within and outside of the government, with the heads of key government departments serving as special invitees. It is an overarching council that assists the PSA's office in understanding challenges and formulating interventions.

The empowered Technology Group (ETG), chaired by the PSA, comprises the heads of Atomic Energy Commission, Space Commission, DRDO and the departments of Electronics & Information Technology, DoT and DST, the ETG is further supported by a Technology Advisory Group (TAG) comprising of experts from academia and industry. It operates on three main pillars: Policy Guidance, Procurement Support, and R&D Support.

India has also followed the practice - now less frequently observed - of constituting expert panels to provide guidance on technology governance. Some examples include the AI Task Force in 2017, Justice B.N. Srikrishna Committee in 2018 and Non-Personal Data Governance Framework Committee in 2019.

Traditionally, the Indian government has relied heavily on the expertise available in public academic institutes for support with expertise in emerging technologies. Institutions such as the Indian Institute of Science (IISc) and the Indian Institutes of Technology (IITs) have long served as key knowledge partners for various ministries and departments. Whilst there has been a gradual openness in government for collaboration with private academic institutions, such engagements remain limited.

As Indian industries continue to mature and increasingly match global standards, they have developed significant expertise across various emerging technologies. This growing technical capacity positions them well to provide informed, strategic support to the government in shaping technology-related policies. Traditional industry bodies like Confederation of Indian Industries (CII), Federation of Indian Chambers of Commerce & Industry (FICCI) and Associated Chambers of Commerce and Industry of India (ASSOCHAM) continue to support the government in various policy-making aspects and have constituted sector-specific wings. Meanwhile, sector-specific industry bodies

in domains of emerging technologies, like the National Association of Software and Service Companies (NASSCOM) in IT, the Data Security Council of India in cybersecurity, the Association of Biotechnology Led Enterprises (ABLE) in biotechnology and the Indian Space Association (ISpA) in space, are actively involved in policy advocacy and offering support to the government with policy formulations.

The Indian government, historically, has collaborated primarily with government-funded think tanks for policy research, advisory support as well as technology assessment. However, the advent of privately funded think-tanks in the last couple of decades has contributed to the policy discourse by introducing independent perspectives, diverse skill sets and a multi-disciplinary approach. While their involvement varies in scale and formality, think tanks increasingly shape the narrative and substance of technology governance, particularly in areas where institutional capacity within the government is still evolving.

4. Case Studies

In this section, we provide a brief analysis of the prominence of TIA in the development of policy in Australia and India addressing the impacts of four technology classes: (1) nuclear accident management, (2) AI, (3) aerial drones, and (4) advanced telecommunications (5G and 6G). For each technology chosen, we offer a brief overview of the international interests that are engaged from the point of view of peace and stability. We comment briefly, as appropriate, on the benchmarks we identified in the report for understanding what might constitute an advanced TIA, as opposed to basic or intermediate. These are: the depth and granularity of specialist input; recognition of the central place of the non-technical social, political, and economic impacts; breadth and depth of stakeholder input; the comprehensiveness of analysis, including international and alternative views; timeliness; and high relevance to policy for peace and stability.

4.1 Nuclear Accident Prevention and Management

For both Australia and India, their cooperative security policies for peace and stability have accorded nuclear issues an extremely high priority according to distinct national interests. Both have given a high priority to technologies that can either prevent nuclear accidents or mitigate their impact. The two countries have addressed these quite differently and we have chosen two distinct case studies that are linked by those policy challenges. For Australia, we have chosen the case of technology assessment for safety regimes and detection technologies associated with nuclear powered warships and submarines. For India, since it operates civil nuclear reactors, with 24 in operation and 18 more under construction or being planned, we have chosen the case of cyber security in nuclear plants.

Nuclear technologies have been a topic of cooperative diplomacy in support of peace and stability for at least six decades, as manifested in the creation of the International Atomic Energy Agency (IAEA) in 1957 and the Nuclear Non-Proliferation Treaty of 1967. (For links to nuclear disarmament treaty texts in one location, see UNODA, n.d.). Australia and India have quite different positions on most of these regimes. For example, a legally binding international treaty on radioactive waste safety, the Joint Convention on the Safety of Spent Fuel Management and on the Safety of Radioactive Waste Management, entered into force on 18 June 2001, with Australia as a party and India not. (For links to nuclear safety treaties in one location, see IAEA 2025.) On the other hand, India has signed a significant number of safeguards agreements with nuclear technology and fuel suppliers, such as the EU India treaty of 2020 (India MEA 2021).

A strong policy foundation for including nuclear safety as a case study in this paper can be found in the nuclear cooperation agreement signed by the two countries in 2014. It is premised on mutual "commitments to achieve the highest standards of radiation and nuclear safety based on a scientific approach, operating experience and best practices, as well as to ensure that the use of radiation and atomic energy in all its applications is safe for the health of radiation workers, members of the public and the environment" (Department of Foreign Affairs and Trade 2014, p. 2). In Article II of the agreement, there is specific mention of cooperation in "Technological Advancements". The text of the agreement recalls the several multilateral treaties on nuclear safety to which both countries are party: the Convention on Nuclear Safety, signed in 1994; the Convention on Assistance in the Case of a Nuclear Accident or Radiological Emergency, signed in 1986; and the Convention on Early Notification of a Nuclear Accident, also signed in 1986.

While nuclear technologies themselves do not figure in the typical lists of critical technologies issued by either Australia or India, the two governments depend on emerging and critical technologies in relation to management and security of nuclear materials. This is a well-researched topic and covers fields like "advanced surveillance and monitoring systems, cybersecurity and digital protection, non-destructive evaluation techniques, physical security enhancements, [and] nuclear material .... forensics" (Shubayr 2024). The IAEA International Conference on Nuclear Security (ICONS) in 2024 dedicated a plenary session to the impact of emerging technologies. The head of the Australian

Government's Safeguards office was a lead presenter in that session and later identified emerging technologies, such as "artificial intelligence, autonomous systems and quantum technologies", as important to nuclear security and relevant international regimes (Australia ASNO 2024, p. 15).

4.1.1 Australia

Statements by the Australian Government on critical technologies policy first established in 2020 do not make any references to nuclear power or the prevention of nuclear accidents involving nuclear-powered ship visits. On the other hand, the government has always regarded these issues as the highest policy priority, essential or crucial. The 2024 statement from the head of ASNO on critical technologies mentioned above makes an explicit connection between critical emerging technologies and nuclear safety.

Between 1985 and 2025, Australia has been engaged in public-facing assessments of nuclear-related technology impacting its own defence policies, as well as the stability of global regimes and regional arrangements. The defining aspect of these assessments was the potential impact on the Australia/US military alliance that has been in place since 1955 under the ANZUS Treaty. The public-facing assessments, conducted mostly by the national parliament, were complemented by many internal government analyses (which have rarely been shared in any detail with the parliament or the public).

The nuclear issues that have forced the pace on national sentiment have been recurring though with c less intensity as time wore on:

- export of uranium
- possible development of nuclear power stations in Australia
- visits by nuclear-powered warships
- creation of the South Pacific Nuclear Weapons Free Zone under the Treaty of Rarotonga (signed in 1985), latest signatory 5 March 2025
- safety aspects of the acquisition by Australia of nuclear-powered submarines under the 2021 AUKUS agreement.

This short case study does not address all of these reference points but concentrates on community safety aspects of the presence in Australia of nuclear-powered and nuclear armed warships in the mid-1980s and review after 2021 of the community safety aspects of nuclear fuels used in submarines operated by Australia, the US or the UK.

The report from the Australian parliament on contingency planning for safety aspects of nuclear-powered or nuclear-armed warships to Australia (Australia Senate, 1989) has been the most compelling example of stakeholder consultation in Australia for TIA in support of peace and stability. The inquiry over three years by the Senate Standing Committee on Foreign Affairs, Defence and Trade, received 102 submissions from the community, specialists and government. The investigation was not rushed; it undertook extensive stakeholder and specialist consultations, and it was comprehensive, with the report extending to more than 600 pages.

The stated aim of the inquiry when it began in 1986 was to develop standard procedures to apply throughout Australia for safety management during visits of these warships. The Committee proceeded on the basis of a mission to educate the Australian public, since it believed that there was a "widespread lack of accurate information in the Australian community on the subject matter of the inquiry" (Australia Senate 1989, p. 7). The real agenda was of much higher strategic significance as discussed below. Another reason for including this as a case study is that the Committee recommended a continuing process of TIA in support of ongoing emergency planning:

> "the Commonwealth Government produced a document containing all the necessary scientific background on naval nuclear reactors; the nature of the potential hazards resulting from accidents involving the reactors which the plans have to address; and other background information which is common to all the plans. The document should be suitable for incorporation in, or attachment to, individual port safety plans" (p. xiii).

One purpose of the inquiry, from the point of view of the major political parties, was to defuse negative public attitudes in Australia to the nuclear aspects of the Australia-US military alliance. Another purpose, and one that fits the peace and stability focus of this paper very well, was to shore up positive attitudes in the South Pacific region toward the continuation of visits by nuclear-powered warships (NPW) or ships carrying nuclear weapons, or transits of such ships through the maritime areas of the region.

The inquiry established political acceptance of a continuing need for review of nuclear safety technologies, both in support of a stable international order and to address persistent community concerns, around visits by such warships. The "Defence Operations Manual (OPSMAN 1) Visits to Australia by Nuclear–Powered Warships" is still in force though with revisions, having codified the Senate report's recommendations. These included a 42-day advance notice for NPW visits to allow safety preparations and to regularise mandatory interventions by state-led port safety organisations during the visits. The Environmental Radiation Monitoring Program recommended by the report became mandatory. This involved pre-visit baseline measurements of natural radiation; real-time gamma radiation detection activity during visits; and post-visit seawater and sediment sampling to detect releases.

The continuing relevance of this TIA is demonstrated by the fact that in 2023, the Australian Department of Defence reissued its latest version of the official policy on managing such visits: "Defence Operations Manual (OPSMAN 1)" (Australia Defence 2023). The update reflects assessments of improvements in technology for radiation detection.

The main limitation of the inquiry was budgetary. Senate committees had not previously undertaken an inquiry of such magnitude. Each committee only had a staff of around three to five, usually none specialised in the work of most inquiries. Expenses for the work usually only covered a small number of committee hearings, commonly held in selected state capitals and the national capital, and occasional support to one or two specialist consultants with appropriate expertise. To augment the limited expertise on nuclear matters within the small staff, the Committee appointed two technical specialists to assist it: the Head of the Nuclear Plant Safety Unit in the Australian Nuclear Science and Technology Organisation (ANSTO), and a naval officer. Both served as channels for the flow of specialist information from their agencies to the Committee.

Their expertise was supplemented by the specialist knowledge available to the Committee through research by the very small Secretariat of 2-3 non-specialist people and by the specialist opinion contained in a number of the submissions to the Committee. The quality of the final report was due in no small part to the meticulousness of the small committee staff and the dedication of the small number of Senators serving on the committee in 1988 through to 1989. None of them were specialists in the field. Nevertheless, as mentioned above, the report has shaped Australia's safety frameworks for visits by these warships to the present day, including through continuous reassessment. Its recommendations led to rigorous risk assessment protocols, enhanced monitoring systems, and institutionalised interagency coordination. There have been a number of direct and enduring influences of the report. For example, the report probably contributed to the creation in 1999 of the Australian Radiation Protection and Nuclear Safety Agency (ARPANSA), which became the regulatory authority of nuclear technologies, leaving ANSTO to concentrate on missions related to management of the nuclear sector.

The political context of the inquiry helps understand the forces driving it and the need for it to include fine technical detail, which has not been common in parliamentary committee reports. After national elections in 1987, the Australian Senate had two members of the Nuclear Disarmament Party, which was a focal point for opposition to visits by these nuclear related warships. The Committee was under pressure to deliver a report that would neutralise such opposition. Over several years prior, the Australian government had taken a leading role in developing the Treaty of Rarotonga for a Nuclear-Free Zone in the South Pacific, signed in 1985, to try to defuse escalating opposition at home and in the regions to the ship visits. In 1984,

Australia's only formal multilateral military alliance, ANZUS, began to unravel after New Zealand banned nuclear-powered and nuclear-armed warship visits, leading to the suspension by the US of its security guarantee to New Zealand. In 1985, French secret service agents bombed and sank the Greenpeace boat, *Rainbow Warrior*, in Auckland harbour prior to its planned departure for a protest at the French nuclear weapons testing site at Mururoa atoll in the French territory of Polynesia.

The assessment of nuclear safety became the subject of further parliamentary inquiry several times after 1989 in the Joint Standing Committee on Treaties (JSCT) for the review of several safeguards agreements and other treaties touching on nuclear safety. The inquiries involved some public consultation (Australia Parliament 2001). JSCT did review the 2014 Australia India nuclear cooperation agreement (Australia Parliament 2015).

The most notable set of subsequent deliberations given the impact of the 1989 Senate committee report came in 2024, also in the Joint Standing Committee on Treaties looking at Australia/US nuclear powered submarines (Australia Parliament 2024). The time frame for the inquiry was truncated. On 12 August 2024, the Committee invited submissions to be made no later than 2 September 2024. This was an extremely short time frame for review, considering the gravity of the issues being addressed. It received 260 submissions and delivered its report in November. The 2024 report (p. 5) noted the grave sensitivity of some aspects of its inquiry, especially naval nuclear propulsion information and technology, and "therefore the maintenance of mutually determined information security policies". On the other hand, the Committee called for the government's approach to nuclear waste to be as transparent and consultative as possible (p. 27).

While supporting the conclusion of the AUKUS Treaty, the Committee recommended that the government elevate the priority attached to "community and worker consultation, engagement and public transparency" as it developed plans for managing, transporting and storing nuclear waste from the submarines (Australia Parliament 2024a, p. ix). It also recommended that the government make public "advice published by the Australian Naval Nuclear Power Safety Regulator ... within a timely fashion to enhance transparency" (p. ix).

In releasing this report, the Committee Chair, Lisa Chesters MP, emphasised the need for continuous public information by the government and continuing parliamentary scrutiny (House of Representatives 2024). Chesters said the aim would be "to include expanding and enhancing community education activities to inform the community on how AUKUS will benefit Australia and help to dispel a number of emerging AUKUS myths".

There is a stark difference between the way in which the Treaties Committee conducts its work, which is normally just a few months in each case, and the ways in which a Standing Committee can operate, usually taking more than a year in more complex cases, as in the 1989 report on visits by nuclear powered warships.

The report also made several references to the international legal commitments of Australia in this field, thereby underscoring the continuing high relevance of the peace and stability diplomacy to management of nuclear materials inside Australia.

Thus, we can conclude that the Senate report of 1989 on safety of nuclear power warships is probably the closest Australia has come to an advanced level of TIA on a critical technology affecting peace and stability. On the basis of the 2024 report, we can also conclude that the parliamentary committees remain an important reference point for Australian TIA especially with regard to stakeholder consultation and foundational ethical approaches.

4.1.2 India

India's cooperative diplomacy in the nuclear sphere is multi-dimensional. For this paper we look at TIA for the cyber security of Indian nuclear facilities as a topical case study. An Indian think tank has assessed cyber technologies, and the emerging innovations in them as "having the highest probability of threat to nuclear security", just ahead of "insider threats, which can arise from cybersecurity breaches" (Rajagopolan et al. 2024, p.25). The report specifically mentioned innovations outside cybersecurity: "radiation detection, and emergency response systems offer capabilities to pre-empt,

detect, and mitigate potential risks" (p. 49). Numerous Indian sources, including the government and policy researchers, have highlighted the central role of diplomacy in mitigating the cyber risks to nuclear stability (see for example Saikhu 2024).

India participated in the Nuclear Safety Summit in 2014 at the Hague, at which a policy paper was presented on the importance of enhanced cyber security at nuclear power plants, including through a peer review process led by the International Atomic Energy Agency (IAEA) (Austin et al. 2014). In 2015, India volunteered for an IAEA review of safety of its civil power generators (IAEA 2015). There is a public report of the assessment, but it does not mention cyber security, though the peer review process at that time certainly had the option of including cyber security assessment. A report from an Indian think tank around that time, had paid considerable attention to cyber threats in the nuclear sector (Rajagopolan et al 2016). It reported such threats were being "addressed by the Computer Information and Security Advisory Group (CISAG)" (p. 50). There is almost no information in the public domain about cyber security in India's civil nuclear sector at that time.

The IAEA does not appear to have conducted a peer review or inspection of cybersecurity at Indian nuclear plants. India's several IAEA peer reviews have focused on physical and operational safety, not cyber threats.

After a North Korean cyber attack on a civil nuclear facility in 2019, the Indian government undertook a number of reassessments of the cybersecurity of its nuclear systems (India Rajya Sabha 2022). We can presume that this would have included the potential of new hacking technologies, including AI-based tools. Measures assessed by the Indian government included "authorisation, authentication, and access control techniques, stringent configuration management, and surveillance", as well as "improving internet and administrative intranet connectivity, restricting the use of portable devices, and limiting access to specific websites and IP addresses". The agency leading the assessments was the Computer & Information Security Advisory Group (CISAG) – DAE, supported by the Indian Computer Emergency Response Team (CERT-In).

According to the DAE, the cyber security infrastructure in India's nuclear facilities follows design principles and guidelines set up by the Task force for Instrumentation and Control Security (TAFICS), the CISAG, and CERT-IN (India DAE 2022). These agencies rely ultimately on standards and guidelines that are derived in large part from IAEA standards. The government has undertaken a range of other measures. For example, in 2021, the Ministry of Power issued the Central Electricity Authority (CEA) Guidelines that mandated cyber security plans (CSP) for all power-generating facilities, including nuclear plants (India CEA 2024). But it has not released a single in-depth report assessing the impacts of cyber technologies on nuclear safety. Its output is mainly through sectoral guidelines, such as CEA 2021, and internal audits. CISAG-DAE conducts audits, but findings remain classified. There have been authoritative reports from elsewhere (Mallick 2019; Mohan 2021), but few would meet the standards of wide public consultation envisaged in a typical TIA. CEA further issued draft regulations for cyber security in the power sector in 2024 (India CEA 2024) soliciting public feedback. But there is no information available on the Authority's conducting wide-ranging stakeholder consultations since that time.

There would appear to be considerable room for India to undertake more public-facing TIA for the effects of critical and emerging technologies on nuclear safety given the grave consequences for of a major nuclear accident for community safety, national security and India's peace and stability diplomacy.

4.2 Artificial Intelligence

AI as a technology category has many subfields which present distinct challenges for TIA. The more established subfields include machine learning (ML), computer vision, and natural language processing (NLP). Emerging subfields include reinforcement learning (RL), generative AI, and self-supervised learning. Frontier sub-fields include cutting-edge innovations such as neuromorphic computing (brain-inspired hardware) and federated AI (decentralized learning). AI applications often rely on the integration of several of these subfields. Most countries regard AI as a potentially decisive technology for many fields of endeavour, including the diplomacy of peace and stability. In almost all countries, the practice of TIA to address the many

applications of these diverse subfields of AI is a recent and still maturing undertaking, to the extent it exists at all.

Subfields can be distinguished by the type of AI technology used, such as those named above, or by the purpose. For assessment of impact, a focus on the purpose or mission of the use of the technology may be more important. Table 4 lists different examples of such a purpose for peace and stability. The list suggests that TIA in the field of AI for peace and stability will be granular as to the purpose and sub-technologies of AI used. Generalised studies that assess the potential influences of AI on international security are assessing potential and not impact.

Table 4: Current uses of AI sub-technologies for a Peace and Stability Purpose

AI Sub-Technology / Machine	Application for Peace & Stability
AI-enabled satellite imagery analysis	Monitoring ceasefire lines, arms movements, disaster impacts
AI-powered early warning systems	Predicting conflict outbreaks, resource-driven disputes
non-weaponised surveillance drones	Monitoring ceasefire violations, peacekeeping patrols
AI-based social media monitoring	Detecting hate speech, disinformation, incitement to violence
automated ceasefire monitoring sensors	Acoustic/visual sensors to detect gunfire or explosions
AI-driven humanitarian logistics platforms	Optimising aid delivery in conflict/post-conflict zones
AI-enabled facial recognition for access control	Securing peacekeeping bases, refugee camps
AI-powered cyber defence systems	Protecting critical infrastructure from cyber attacks
AI-assisted document analysis	Supporting arms control treaty verification, open-source intelligence
AI-driven environmental monitoring platforms	Detecting illicit mining/logging that is funding violent actors
AI-enhanced mine detection robots	Clearing landmines for civilian safety
AI-based disease outbreak prediction	Preventing health crises in fragile states
AI-enabled border surveillance (non-lethal)	Monitoring migration, trafficking, and arms smuggling
AI-driven data fusion for situational awareness	Integrating multisource data for peacekeeping operations
AI-based human rights violation detection	Analysing media, satellite, and social data for abuses
AI-assisted crisis mapping platforms	Real-time mapping of violence, displacement
AI-enabled emergency communication bots	Disseminating verified information in conflict zones
AI-powered supply chain tracking	Monitoring conflict minerals, arms embargo compliance

Sources: Amani Africa (2025); SIPRI (2025); Tuvdendarjaa (2025); DigitalDefynd, (2024): Arms Control Association,(2024); Giovanardi (2024)

4.2.1 Australia

The national parliament has been the main source of public-facing impact assessment of AI at the whole-of-country level in Australia. While other efforts have been substantial, they have focussed on selected aspects, few of which come under the purview of peace and stability as defined in this paper. The main exception is Australian diplomacy related to potential international regimes regulating lethal autonomous weapons systems (LAWS). Domestically, the Department of Industry, Science and Resources has developed and is responsible for Australia's voluntary AI Ethics Principles. On the diplomatic front, Australia supports the OECD Principles for trustworthy AI adopted in 2019 and updated in 2024 (OECD 2024). Australia supports

the Global Partnership on AI (GPAI) of which it was a founding member in 2020.

Prior to 2024, Australia's approach to technology assessment for AI was characterised by an evolution from sector-specific pilots and risk frameworks toward coordinated, whole-of-government policies and independent oversight. This included work by the Australian Taxation Office (ATO), the Digital Transformation Agency (DTA), and the Commonwealth Scientific and Industrial Research Organisation (CSIRO). The quality of part of that effort was assessed by the Australian National Audit Office (ANAO) in a review of the ATO, judged to be the most advanced civil sector organisation in its use of AI (Australia ANAO 2025). The Report found a number of gaps in assessment and subsequent regulatory effort (p. 6). For example, by August 2024, the ATO had only completed data ethics assessments for 26% of its AI models in use. The audit recommended improvements in risk management, information management, and the development of a comprehensive AI policy (pp. 12-13).

In October 2024, the Digital Transformation Agency (DTA) released a pilot AI assurance framework to guide agencies through the impact assessment of AI use (Australia DTA 2024). The framework, piloted across government agencies, outlined when and how to conduct impact assessments, including criteria based on project cost (over $10 million), their potential for more than insignificant harm, the potential for materially influencing decision-making, and the absence of human review for key outputs. The discussion of risk factors in the guidelines is directed to human impacts of the sort that the basic concept of TIA emerging in the 1970s in the US was intended to address. It laid the groundwork for more systematic, risk-based TIA across government as a normal part of assurance processes for AI systems.

The first major report addressing whole-of-country interests came when the Senate Select Committee on Adopting Artificial Intelligence (AI) issued its final report in November 2024, focusing on the negative influence of high-risk applications on democracy and workplace safety, as well as intellectual property rights (Australia Senate 2024a). The committee received 245 public submissions and held six public hearings, all but one in Canberra. One of the many forms of AI which it identified as relevant to its inquiry was AI frontier models: "capabilities that could severely threaten public safety and global security" through the design of chemical weapons, exploiting vulnerabilities in safety-critical software systems, or synthesising persuasive disinformation at scale. In its submission to the inquiry, the Department of Home Affairs saw severe national security risks presented by AI (Australia Senate 2024a, p. 168). The main civil service trade union made a specific proposal (p. 56) for creation of a federal parliamentary Office of Technology Assessment. The report made 13 recommendations covering the need for transparent AI impact assessments, stronger ethical and legal guardrails, greater public engagement and education, and support for innovation balanced by risk mitigation (Australia Senate 2024a, pp. xv-xvi).

The same committee on AI also published an Interim Report in October 2024 exploring how generative AI could influence electoral processes and undermine public trust in democratic institutions, including through algorithms fostering divisiveness in the country (Australia Senate 2024b). It examined regulatory gaps and proposed policy responses, such as mandatory guardrails for high-risk AI applications and voluntary labelling of AI-generated materials. It assessed that generative AI tools enable foreign actors and malicious entities to create "realistic though artificial content intended to deceive the public" at unprecedented speed and scale, exacerbating risks to social cohesion.

The Parliamentary Joint Committee on Intelligence and Security reported on its review of the use of AI by Australian intelligence agencies at the request of the Australian government as part of the Committee's annual review of the administration of the agencies for the 2022–23 financial year (Australia Parliament 2025a). The AI aspects of this inquiry did not involve consultations with public interest groups. The submissions received from intelligence agencies, supplemented by reports from the IGIS and ANAO, were classified and therefore not publicly available. However, the Inspector-General of Intelligence and Security (IGIS), ONI, and ANAO publicly released unclassified versions of their submissions. The terms of reference required the committee to review, inter alia:

- ethical and responsible management of AI, ML and Bio Intelligence systems
- strategic workforce planning

The Joint Committee of Public Accounts and Audit (Australia Parliament 2025b) issued a report in 2025, titled "Inquiry into the Use and Governance of AI by Public Sector Entities: Proceed with Caution" (Australia Parliament 2025b). It focused on the governance of AI systems in Commonwealth entities, highlighting risks such as inadequate datasets, biases, disinformation, and sovereign risks. The inquiry received 46 submissions and 11 supplementary submissions containing responses to questions from the Committee or taken on notice at public hearings. The Committee held two public hearings.

Its report, "Proceed with Caution", noted (p. 41) that "disinformation, propaganda and foreign interference, and electoral interference" are important risks that arise from the use of AI. The final recommendation was for the parliament to establish a "statutory Joint Committee on Artificial Intelligence and Emerging Technologies" for it to have fully effective oversight of how the Government and the APS are managing the impacts of AI. Submissions to the committee referenced AI's dual-use potential in defence and cyber warfare, the impact of autonomous weapons systems in lowering thresholds for conflict escalation, reduced human oversight in targeting decisions, and the risks of algorithmic bias misidentifying civilian infrastructure.

The committee's process included extensive public submissions, expert testimony, and analysis of international best practices. It highlighted the lack of a "clear APS-wide picture" of AI deployment and called for coordinated, transparent reporting and assessment mechanisms across the public sector (Australia Parliament 2025b, p. 10). The committee noted that while agencies like the ATO and CSIRO had adopted AI for tasks ranging from compliance to disaster prediction, there was no consistent, sector-wide approach to technology impact assessment or risk management.

Australian academic and think tank analysis of AI impacts on peace and stability has been substantial, though somewhat focused on electoral misinformation, erosion of institutional trust, and foreign interference. Policy recommendations have addressed legal reform to ensure AI systems serve the public interest, particularly in education, employment, civic participation and the development of frameworks to prevent AI from undermining democratic processes.

There appear to be unaddressed community anxieties about AI. A University of Queensland survey found that 80% of Australian respondents ranked AI's catastrophic risks (e.g., cyberattacks, unemployment) as significant risks, alongside pandemics and nuclear war (Noetel, Saeri, Graham 2024). The survey uncovered several disparities between public and government priorities. The Australian Institute of International Affairs warns that advanced AI could become a "synthetic WMD" through cognitive warfare: AI-driven propaganda altering human belief systems at scale.

The closest Australia has come to TIA for AI affecting peace and stability has been its involvement in international deliberations for control of lethal autonomous weapon systems (LAWS). The process has included substantial and regular consultation with or submission from Australian specialists and interest groups, for example, the Australian Human Rights Commission. This is a continuing set of activities. An overview can be found in the Inquiry into the Defence Annual Report 2022-23 with Chapter 5 dedicated to AI and LAWS (Australia Parliament 2024b).

While the government opposes proposals for new treaties to govern LAWS, Australia has participated in all formal UN meetings since 2016 and has hosted cross-regional expert meetings in Sydney to share best practices on legal aspects. Australia prioritises its alliance interests over more internationalist perspectives proposed by some domestic interest groups, such as the Human Rights Commission (a statutory body completely independent of the government).

Australia appears to have undertaken only modest levels of TIA on AI where multi-stakeholder perspectives and public facing engagement have been prominent, and that is especially the case for matters affecting peace and stability. While numerous analyses have been published by Australian specialists, policy analysts and business interests, the

scope has been rather general and focused more on potential than on observed impact.

4.2.2 India

India's large and prosperous ICT economy has led it to move robustly on developing frameworks for assessments on diverse aspects of AI. The bulk of the effort has come from government agencies and some industry groups.

In June 2018, the government's premier policy research centre, the National Institute for the Transformation of India (NITI), which had replaced the Planning Commission set up in 1950, published "The National Strategy for Artificial Intelligence" (NSAI), suggesting that it was a foundation study for India's efforts that would need wider consultations and consensus building to further develop (India NITI AAYOG 2018, p. 7). This set the tone for a comprehensive consultative approach to the assessment of the potential for AI in India and principles of its use. While preparing this report, there was substantial consultation with specialists, including from the domestic and international private sector. NITI AAYOG undertook a pilot analysis in sectors like health and agriculture. It declared that India's "strengths and characteristics" would help position it "among leaders on the global AI map" (India NITI AAYOG 2018, p. 5). The NSAI set the goal of being a national leader in developing ethical approaches for the use of AI and committed itself to working with a diverse group of stakeholders, including socialists, officials, the commercial sector, public sector organisations, and citizens.

Following the practice of other leading countries, NITI AAYOG published the Principles of Responsible AI (India NITI AAYOG 2021), laying out seven broad principles: (1) safety and reliability; (2) inclusivity and non-discrimination; (3) equality; (4) privacy and security; (5) transparency; (6) accountability; and (7) protection and reinforcement of positive human values. The attention to transparency, privacy and human values set the scene for future technology assessments to be consultative and multi-stakeholder. NITI AAYOG published several additional guideline papers, such as Operationalising Principles (India NITI AAYOG 2021). The paper focused on the role of government intervention to drive responsible AI adoption in social sectors, in partnership with the private sector and research institutes.

One example of the sort of TIA for AI that India was set to undertake was released in 2022 and it was the first use case undertaken by India: "Responsible AI for All: Adopting the Framework – A use case approach on Facial Recognition Technology" (India NITI AAYOG 2022, p. 1). The report revealed consultations with some private sector interests and government agencies (pp.-iii), but this was on a very limited scale. There was little effort to establish a broader set of stakeholders.

The IndiaAI Mission is the government's flagship programme for strengthening India's AI ecosystem and has a budget outlay of Rs 10,372 crore (A$161 million) across its seven pillars (India MeitY 2024a). A significant share, around 44%, is directed toward building domestic computing capacity. An innovation centre and startup financing each account for 19% of the budget, while the remainder is distributed among future skills, an application development initiative, a datasets platform, and a safe and trusted AI initiative. Some of these focus on building domestic computing capacity and indigenous models addressing Indian use cases, which seem to be a response to the influence of geopolitical developments such as restrictions on export of chips and AI models.

To coincide with the launch of the IndiaAI Mission, MeitY, in collaboration with UNESCO, organised a series of multi-stakeholder workshops across the country on different aspects of the IndiaAI Mission (India MeitY 2024b).

There is a lack of comprehensive regulation in India for managing the broad risks associated with AI. In 2024, the office of the Principal Scientific Advisor (PSA) set up a multistakeholder Advisory Group including representatives from relevant ministries (IndiaAI 2025, pp. 1-2). The Advisory Group was tasked with providing guidance on AI governance and offering insights for the necessary regulatory oversight to enable sustainable and ethical development of AI technologies. Under the guidance of the Advisory Group, a Subcommittee on 'AI Governance and Guidelines Development' was constituted to provide actionable recommendations for AI governance in India. The Subcommittee's man-

date was to examine key issues related to AI governance in India, conduct a gap analysis of existing frameworks, and propose recommendations for a comprehensive approach to ensure the trustworthiness and accountability of AI systems in India. The sub-committee issued its first guidelines in 2025 to initiate a comprehensive multi-faceted programme of stakeholder consultation engaging government, private sector and community interests. The report on AI Governance Guidelines proposes a Technical Secretariat to enhance state capacity to govern AI and voluntary disclosure and compliance requirements, but its implementation is uncertain (IndiaAI 2025). Institutions such as the Centre for Responsible AI, established at IIT Madras, focus on highlighting the risks and harms of AI adoption (IIT 2023). Overall, while a lot of the state effort is aimed at enabling AI innovation in India, more effort can be directed at building the required governance capabilities and performing technology assessments to anticipate the impact of AI adoption.

The Ministry for Electronics and Information Technology (MeitY), the nodal agency for technology regulation in India has preferred a light-touch approach to AI governance while focussing on creating an enabling environment for innovation (Mohanty and Sahu 2024). Some sectors, such as finance and health, have seen specific regulations and compliance requirements. For instance, the RBI has formed a panel to review AI adoption in financial services, survey best practices in governance globally, and recommend a compliance framework (India RBI 2024). Similarly, the ICMR Ethical Guidelines provide principles for AI development and deployment in healthcare (ICMR 2023). In 2024, NASSCOM launched the Developer's Playbook for Responsible AI in India, which led to a multistakeholder effort to establish a sector agnostic risk mitigation framework (NASSCOM 2024).

In stark contrast to the light-touch approach, an advisory was issued in March 2024 requiring the government's permission before deploying certain AI models in India to prevent algorithmic discrimination and the spread of deepfakes. The advisory drew sharp criticism from the industry about regulatory overreach and was subsequently withdrawn (Barik 2024). This has been attributed to differing views within the government (Mohanty and Sahu 2024). For instance, the Prime Minister's Economic Advisory Council published a report describing AI as a "complex adaptive system" which required proactive regulatory intervention (Sanyal et al. 2024).

More specifically for the peace and stability agenda, India has been highly visible in the UN work on LAWS beginning during the 2014-2016 Informal Meeting of Experts and subsequent Group of Governmental Experts. This has involved multi-sector and specialist consultation through mechanisms established in the defence portfolio, such as the AI Task Force on National Security and Defence, set up in 2018, chaired by N. Chandrasekaran, a leader of Tata Sons, comprising 17 members from the armed forces, academics, government research organisations, and industry, including the National Cyber Security Coordinator. With a remit for military development, it also addressed dual use aspects. It led to the creation of a Defence AI Council which has overseen a variety of technology assessments, including ethics and algorithmic accountability. There has only been a limited amount of consultation with civil society. Beyond the works on LAWS or on AI-enabled facial recognition, there appear to be no prominent multi-stakeholder public-facing analyses in India with any granularity on the impact of AI subfields on peace and stability.

4.3 Aerial Drones

The rapid take-up of aerial drone technology and its many impacts on peace and stability make it an ideal candidate for a case study of TIA for a critical emerging technology, albeit one whose novelty and criticality is due more to newly-devised applications than to breakthroughs in basic science. One set of breakthroughs that has mattered with drones is, as noted above in Table 4, the expansion of uses associated with AI. Drones certainly affect peace and stability diplomacy, which includes international regimes as well as the protection of international obligations on civil and political rights. A clear indication of this can be seen in the advocacy of the regulation of drones in maintaining the peace and stability objectives of the Antarctic Treaty (Chen and Wu 2024). Another international regime where drones have been regulated for peace and stability is in the model safety regulations for uncrewed aerial systems (AUS) adopted by the International Civil Aviation Organisation (ICAO 2014).

4.3.1 Australia

The introduction of aerial drones, also known as uninhabited aerial vehicles (UAVs), into the Australian landscape attracted attention from defence, government agencies, regulating bodies, large commercial organisations, non-government organisations, the media and citizens. Australia was one of the first countries to regulate remotely piloted aircraft systems (RPAS) in 2002, with the Civil Aviation Safety Authority (CASA) introducing legislation under Civil Aviation Safety Regulations Part 101 (Norton Rose Fullbright 2016). Foundational technology assessments involving widespread consultation and comprehensive technical analysis do not appear to have been undertaken at the time.

CASA continued to introduce significant amendments to rules with respect to drone operators (Clarke & Moses 2014), such as in September 2016 to cover all recreational, sub-2 kg commercial, and commercial drone operations. There has been continued pressure on CASA to regulate drones as significant advances in the technology have been made, and they are also widely accessible, while the price of autonomous drones has markedly dropped, making them affordable by a greater number of entities. But CASA primarily focuses on safety and airspace management, and aspects relating to peace and stability have been addressed in occasional references in inquiries by parliamentary committees.

The earliest inquiry was by the House of Representatives Standing Committee on Social Policy and Legal Affairs (Australia House of Representatives 2014). It focused on domestic regulation and privacy issues. One submission raised the positive impact on safety of reporters in war zones (p.10). The report explicitly excluded from its purview military uses (p. 3), going so far as to use the term "remotely piloted aircraft" instead of "drones". This decision was made at industry arguing to avoid association with the US policy of targeted killing using drones (p. 4).

The first public-facing and broadly consultative TIA into international security aspects of drones affecting peace and stability came in an inquiry from the Senate Foreign Affairs, Defence and Trade References Committee (Australia Senate 2015) into Defence use of uninhabited platforms. The Committee received 25 formal submissions, including from industry, federal government departments, state governments, academics, think tanks, ethicists and the International Committee of the Red Cross. It held several public hearings in Canberra.

The committee considered the impact of drones on international humanitarian missions and peacekeeping missions (Australia Senate 2015, p. 32). It recommended to the government that because Australia "continues to have an important role in international disarmament and arms controls regulation to promote global peace and security", the government should "form and advocate a considered position which supports the eventual establishment of international regulation on the use of lethal force" by autonomous weapons systems" (p. 70). Related topics on the impact of drones on peace and stability remained prominent in public discourse since that time (Wiedemann et al. 2023; Howie 2025; Hardy 2025).

The use of both private and commercial drones has particularly sparked considerations around privacy (e.g., matters of consent), potential harms (e.g., drone accidents, noise pollution), potential threats (e.g., cybersecurity), disruptions (e.g., job displacement), and risks (e.g., drone payloads and unauthorised surveillance). Benefits were also considered given the vast Australian landscape, where drones could be used in agriculture and mining, and for emergency services and logistics.

In 2024, the Department of Infrastructure, Transport, Regional Development, Communications and the Arts conducted a privacy impact assessment (PIA) for both recreational drone operators and commercial operators, creating Drone Privacy Guidelines (Australia. Infrastructure 2024). This has been driven mainly by modern drones and their capabilities to capture high-resolution imagery and data from public and private spaces. The OAIC has been exploring the impact of this technology on a variety of legislation, including the Australian Privacy Act.

Clarke and Moses (2014) underscored the importance of public consultation and stakeholder engagement in the regulatory process. However,

defence organisations in Australia have not published their technology impact assessments on drones, or anti-drones for that matter, despite the renewed interest since local Australian companies supplied low-cost drones to Ukraine in 2024.

The Defence Science and Technology Group (DSTG), Australia's leading agency for applying science and technology to safeguard national interests, has focused on safety, security, and technological considerations, ensuring that drone integration aligns with Australia's defence and societal objectives. The DSTG is known for collaborating with research and industry partners, nationally and globally. Much of their work is not available in the public domain.

The overall aim of these technology impact assessments of drones should be that they work to support the development of policies, laws and regulations, and technologies that balance innovation with the protection of individual rights and national interests. TIAs are conducted with respect to dual use technology (military and commercial in this instance), to propel the procurement of a technology, in this instance, for peace and stability – as well as war-fighting and a wide range of civil sector purposes.

4.3.2 India

India's approach to TIA in the context of drones has been shaped largely by its national security landscape. Sharing extensive land borders with countries where geopolitical tensions are quite high, India faces persistent risks from the hostile use of drones. These threats include surveillance and reconnaissance of sensitive defence installations, airspace interference, smuggling of illicit materials (such as drugs and weapons) and even kinetic attacks (Patil and Arora 2023).

An initial outright ban on civilian usage of drones in October 2014 exemplified a highly restrictive regulatory stance. However, recognising the advantages of promoting the use of drones, the government initiated the opening of the sector with the publication of Civilian Aviation Requirements (CAR) for Unmanned Aircraft System (UAS) in 2018 that adopted a "no permission, no take-off" (NPNT) stance. This was subsequently further liberalised with the Drone Rules of 2021, and the subsequent establishment of DigitalSky as an online, centralised, easy-to-use platform to manage and regulate drones (UTM Policy Framework 2021).

Public consultations were undertaken by the Indian government in connection with the GCA Guidelines (2018). The Directorate General of Civil Aviation (DGCA) released its first comprehensive guidelines for civilian drone operations in December 2018, following several years of draft circulars and stakeholder feedback (Rajagopolan and Krishna 2019, p. 56). A task force led by the Minister of State for Civil Aviation was set up to develop these guidelines, with inputs from enforcement authorities, security agencies, industry, and technical experts. Security and stability were addressed through requirements for drone registration, operator authorization, and geofencing of sensitive sites.

In 2021, the Ministry of Civil Aviation (MoCA) released the updated Drone Rules 2021 for public consultation, explicitly inviting comments from the public, industry, and other stakeholders (Gupta 2021).

In 2025, new drone rules were issued based on consultations with industry bodies, security agencies, privacy advocates, civil society, and the public. Peace and stability issues were an important part of the updating (InsideFPV Social 2025a). There were references to airspace restrictions, security protocols, and firming up of no-fly zones around sensitive and strategic locations such as borders, defence installations, and nuclear sites. A specialist media source reported that one of the concerns about drone operations near nuclear power stations was cyber security: "Advanced drones can serve as cyber-attack vectors, potentially interfering with the digital systems that control a nuclear plant's operations" (InsideFPV Social 2025b). National security concerns also led to the prohibition of the import of foreign-manufactured drones in 2022, particularly to mitigate risks associated with surveillance and data leakage but also to reduce dependence on external supply chains.

The Ministry of Home Affairs has also established an Anti-Rogue Drone Technology Committee (ARDTC) under the aegis of the Director General of India's Border Security Force, with a mandate to evaluate available technologies for countering

rogue drones and to certify their effectiveness in neutralising such threats (India Lok Sabha 2023).

4.4 5G and 6G

Decisions in Australia and India on the use of China-sourced 5G and 6G wireless technologies have been made largely on the basis of counter-intelligence assessments by each government. The primary consideration has not been threats to peace and stability as such, but rather that banning such technologies would eliminate serious risks to national security, including domestic security. Moreover, the 5G/6G policy of each country has been shaped largely in the overarching intelligence field rather than in one of the single pillars, as illustrated in Figure 1. However, leading firms and technologists have identified important contributions to be made by 6G to communications in remote areas on such a scale as to impact national development and thereby human security, peace and stability (Saarnisaari et al. 2020)

4.4.1 Australia

The Australian intelligence agencies, primarily ASD, led the technology assessments on the government's decision to exclude Huawei from the National Broadband Network (NBN) in 2012. In classified advice to the government, ASIO advocated the ban due to concerns about cyber espionage and Huawei's alleged ties to the Chinese government. The ASIO assessment highlighted vulnerabilities in critical infrastructure. The Director General of ASIO testified to parliament that the decision was based purely on security grounds (Australia Senate 2012, p. 149). The Attorney-General's Department confirmed the ban was a "risk-based decision" informed by security agency advice (BBC 2012).

Later, as the country set about its roll-out of 5G wireless infrastructure, in which Huawei had indicated an interest as a potential bidder, a range of other agencies and actors became involved. There were reviews by a number of agencies and parliamentary committees. Their decisions were driven by concerns over foreign interference risks, espionage, and the legal obligations of Chinese companies under China's National Intelligence Law. This law had the effect of requiring Chinese firms to hand over any foreign information on host countries and their citizens regardless of the laws in the host country.

The Australian intelligence agencies played the leading role in the government's decisions on banning Chinese companies from the 5G Network development in Australia in 2018. The National Security Committee of the Cabinet was the final decision-maker. It relied on a classified review of risks posed by "high-risk vendors" subject to foreign government coercion (Uren and Cave 2018). The ASD Director-General advised the government that 5G architecture made it impossible to mitigate risks if Huawei participated. This technical assessment underpinned the 2018 ban (SBS News 2018). Huawei made a submission to the 2020 inquiry into 5G, suggesting that the ban would inflate costs and delay innovation, but the Committee supported the government's decision (Australia House of Representatives 2020). There appears to have been little penetration in government assessments of the potential economic or welfare interests of business or the community.

So, at one level the government saw important international security interests at stake in the decision on 5G, but at no stage did it really apply the sorts of approach suggested by advanced TIA. An illustration of this is the fact that the UK intelligence community had adopted a broader view that important community interests and international relationships could be preserved while managing or mitigating risks from using the Chinese 5G technology (United Kingdom 2020a). On the other hand, the UK walked away from this position by ordering telecoms providers in the country to replace all Huawei equipment in UK public 5G networks by 2027 (United Kingdom 2020b).

4.4.2 India

In India, to address risks form Huawei, the National Security Council Secretariat, which reports to the Prime Minister's Office, issued the National Security Directive on the Telecommunications Sector (NSDTS), which came into effect in June 2021 (India NSC 2020).

The directive establishes the trusted source and trusted product framework for telecommunications supply chain security. Telecommunications service providers are required to provide details of

the vendors and the products. The vendors are assessed to qualify as a Trusted Source for which the company governance structures, ownership, shareholding and details of manufacturing sites are reviewed. Further, each of the products needs to undergo the Trusted Product certification, where a review of the components, their sources, details of manufacturing facilities, and details of their software development centres is done.

Prior to the NSDTS directive, the Ministry of Finance had issued the Public Procurement Order in 2020 (India Ministry of Finance 2020). This order amended the General Financial Rules 2017 to mandate bidders from countries that share a land border with India (as China does) to require a political and security clearance from the Ministry of External and Home Affairs. This order covered all new procurements for public sector units and public-private partnerships. Although Chinese vendors are not explicitly mentioned, these directives were issued in the aftermath of the clashes with China in Galwan Valley and are an effort to remove Chinese components in critical infrastructure (Agrawal 2024).

While these measures attempt to address security vulnerabilities in critical infrastructure, they focus on sourcing and ownership while overlooking building the overall robustness of the complex technological ecosystems in which these components operate (Goswami et al. 2025).

The case of 5G and 6G is particularly relevant to this paper for two reasons. First, the two governments undertook a modest degree of consultation on the issues behind bans on Chinese telecoms products, and the prospect for further consultations has improved considerably (Reuters 2019). Second, in 2022, the AICCTP funded a bilateral project on "Ethical 6G – Identifying Elements of an Ethical Framework for 6G and Creating Opportunities for India and Australia". The project, now completed, was led by the Centre for Competition, Investment & Economic Regulation (CCIER), partnering with the Australian Risk Policy Institute (ARPI) and the International Institute of Information Technology, Bangalore (IIITB). One of its basic premises was that the development of 6G should remain closely tethered to the goal of "building safe, secure and accessible cyberspace" (CUTS n.d.).

5. Conclusion

Australia and India have well-established capabilities and processes for technology impact assessment in sectors like health, energy and the environment. Both countries accept in principle the need for multi-stakeholder consultative approaches that have been fundamental to impact assessment in advanced liberal democracies for four to five decades. In the field of critical technologies affecting peace and stability, these assets are rarely applied in the two countries, with variable consistency depending on a range of choices about the priority of the subject and the resources available.

The paper situated peace and stability as one of three main pillars of national security policy where TIA are judged by both countries to be important: national defence policy, especially military capabilities and defence diplomacy; domestic security (e.g., counter-terrorism and protection of civil rights); and peace and stability (i.e., the diplomacy of international security regimes, not closely involving the first two pillars).

The paper also remarked that the intelligence functions of national security cross over between all three pillars. The place of critical technologies in intelligence capabilities does not always allow for this neat distinction between the three pillars.

In both countries, the practices of TIA for peace and stability have a lower priority than TIA in the other two pillars. This may help explain why it proved difficult in this paper and the supporting investigations to identify more than a couple of stand-out examples of TIA for critical technologies in the peace and stability pillar in either country.

Nevertheless, the policies of both Australia and India in critical technologies for the peace and stability pillar are relatively new and will need time to be further refined. Neither country has committed to a standing mechanism or set of processes for executing high-quality TIA, or to greater clarity through a set of best practice standards in the field. This paper suggests that doing this would be beneficial, even as we advise against simply emulating the arrangements for TIA in other countries.

Both Australia and India would benefit from the existence of a new centre of gravity for TIA for the peace and stability pillar, separately from other aspects of national security- where secrecy requirements mitigate against public impact analysis. There would appear to be a small set of options for locating such a centre of gravity with a degree of independence from government: the national parliament, a statutory authority, or the national academies.

The paper proposed benchmarks for TIA around three tiers: basic, intermediate and advanced, depending on several metrics:

- 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
- public transparency
- recognition of the principal place of the non-technical social, political, legal and economic impacts
- comprehensiveness of analysis, including international and alternative views
- timeliness
- high relevance to policy for peace and stability
- a clear ethical framework.

In the field of peace and stability, relying on these metrics, we have seen few examples of TIA in Australia or India that might rise above the basic tier.

There is currently a mismatch between the scale and scope of technologies regarded as critical by both countries, and the resources available for professionally assessing their impact on peace and stability. Consideration of low resource availability for TIA for peace and stability is sufficient by itself to dictate rigorous priority setting when it comes to the choice of a technology or technology class to be analysed.

This consideration gives rise to a need to consider burden-sharing between national institutions on a proactive basis. While the normal process of democratic consultation in an advanced TIA creates an opportunity for that burden-sharing, with stakeholders offering their own detailed TIA, that is not happening in practice. Leading organisations that might be expected to offer their own TIA at an advanced level as part of a national effort do not always rise to the challenge.

Nonetheless, given the importance of critical technologies, the need for obtaining wider community support for new policy, and the dearth of fully comprehensive analyses, including for peace and stability, some priority for enhancement of the capacity in this area seems clear. In that process, if international collaboration could be agreed, the payoffs might be very much enhanced. This collaboration potential will be the focus of the second discussion paper in this study.

References Cited

This paper uses a slightly modified Harvard referencing system. To avoid long organisational titles in the in-text citations, we have shortened these where possible with acronyms for the in-text references and the full name in the list of references. For example, "IAEA (2020)" is used as an in-text citation while in the references list, we repeat the short form followed by the full organisational name: "International Atomic Energy Agency".

For attribution of a work cited to the national government or national parliament of any country, we use a format as follows: [Country name]. [short name for Entity] [year]. [Further long name of organisational element]. [Title][other details].URL. For example: "Australia. Parliament. (2025) Joint Committee on Public Accounts and Audit. "Report 510" ... or "India. Lok Sabha. (2025) ....

Akin, A., Bloch, I., Buhrman, H., Calarco, T., Eichler, C., Eisert, J., Esteve, D., Gisin, N., Glaser, S. J., Jelezko F. (2018). "The quantum technologies roadmap: a European community view". *New Journal of Physics,* 20, https://doi.org/10.1088/1367-2630/aad1ea

Ackoff, R. LO. (1994). "Systems thinking and thinking systems". *System Dynamics Review*, 10(2-3), pp. 175-188, https://doi.org/10.1002/sdr.4260100206

ACOLA. (2017). Australian Council of Learned Academies. "The Role of Energy Storage in Australia's Future Energy Supply Mix", Australian Council of Learned Academies. Melbourne. https://acola.org/hs1-energy-storage-australia/

ACOLA. (2018). Australian Council of Learned Academies. "Synthetic Biology in Australia: Outlook to 2030", Australian Council of Learned Academies. Melbourne, https://acola.org/hs3-synthetic-biology-australia/

ACOLA. (2018). "The Future of Precision Medicine in Australia", Australian Council of Learned Academies. Melbourne, https://acola.org/hs2-precision-medicine-australia

ACOLA. (2019). Australian Council of Learned Academies. "The Effective and Ethical Development of Artificial Intelligence: An opportunity to improve our wellbeing". Melbourne, https://acola.org/hs4-artificial-intelligence-australia/

ACOLA. (2020a). Australian Council of Learned Academies. "The Future of Agricultural Technologies." Melbourne, https://acola.org/hs6-future-agricultural-technologies/

ACOLA. (2020b). "The Internet of Things", Australian Council of Learned Academies. Melbourne. https://acola.org/hs5-internet-of-things-australia/

Alkire, S. (2013). "A conceptual framework for human security." Dept. Int. Develop., Univ. Oxford, Oxford, U.K., Working Paper, https://assets.publishing.service.gov.uk/media/57a08cf740f0b652dd001694/wp2.pdf

Agrawal, A. (2024). "NCSC: Ambiguity around cybersecurity resolved". *Hindustan Times*, 17 October. https://www.hindustantimes.com/india-news/ncsc-ambiguity-around-cybersecurity-resolved-101729111377203.html

Amani Africa. (2025) "AI's Impact on Peace, Security, And Governance", 19 March. https://amaniafrica-et.org/artificial-intelligence-and-its-impact-on-peace-security-and-governance/

Arms Control Association. (2024) "Beyond a Human "In the Loop": Strategic Stability and Artificial Intelligence". Issues Briefs. Volume 16, Issue 4, 12 November. https://www.armscontrol.org/issue-briefs/2024-011/beyond-the-loop

ASPI. (2024). Australian Strategic Policy Institute. "Critical Technology Tracker", Available at https://tech-tracker.aspi.org.au/list-of-technologies/

Austin, G. (2024) 'Quantum Sensing: Comparing the United States and China'. International Institute for Strategic Studies. https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/2024/02/iiss_quantum-sensing_022024.pdf

Austin, G., Cappon, E., McConnell, B., Kostyuk, N. (2014). "A Measure of Restraint in Cyberspace: Reducing Risk to Civilian Nuclear Assets", *EastWest Institute*, New York/Brussels/Moscow, January 2014.

Australia. ANAO. (2025). Australian National Audit Office. "Governance of Artificial Intelligence at the Australian Taxation Office." February. https://www.anao.gov.au/sites/default/files/2025-02/Auditor-General_Report_2024-25_26.pdf

Australia. ANOA. (2024). Australian Safeguards and Non-proliferation Office. https://www.asno.gov.au/sites/default/files/2024-10/ASNO%20-%20Annual%20Report%202023-24.pdf

Australia. CPTCO. (2021). Critical Technologies Policy Coordination Office. "CTCPO Action Plan". https://openresearch-repository.anu.edu.au/server/api/core/bitstreams/1f70ee47-7f25-4641-87ed-b6083bca798b/content

Australia. CSIRO. (2020). Commonwealth Scientific and Industrial Research Organisation. "Growing Australia's Quantum Technology Industry". https://www.csiro.au/-/media/Do-Business/Files/Futures/Quantum/20-00095_SER-FUT_REPORT_QuantumTechnologyRoadmap_WEB_200518.pdf

Australia. Defence. (2023) "Defence Operations Manual (OPSMAN 1) Visits to Australia by Nuclear-Powered Warships". Edition 11. https://www.arpansa.gov.au/sites/default/files/documents/2023-07/

Australia. DFAT. (2021) Department of Foreign Affairs and Trade. "Australia's International Cyber and Critical Tech Engagement Strategy". https://apo.org.au/sites/default/files/resource-files/2021-04/apo-nid311927.pdf.

Australia. DFAT. (2023) Department of Foreign Affairs and Trade. "2023-2030 Australian Cyber Security Strategy". https://www.homeaffairs.gov.au/cyber-security-subsite/files/2023-cyber-security-strategy.pdf

Australia. DFAT. (2024). Department of Foreign Affairs and Trade. "Australia's Submission to the United Nations Secretary-General's Report on Lethal Autonomous Weapons Systems RE: ODA-2024-00019/LAWS | May 2024". https://docs-library.unoda.org/General_Assembly_First_Committee_-Seventy-Ninth_session_(2024)/78-241-Australia-EN.pdf

Australia. DHA (2024). Department of Home Affairs. "Critical technology - enhanced visa screening measures".. https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/critical-technology

Australia. DISR. (2023) Department of Industry, Science and Resources. Australia. (2023) "Critical Technologies Statement". https://www.industry.gov.au/publications/critical-technologies-statement

Australia. DISR. (2023). Department of Industry, Science, Energy & Resources. "List of Critical Technologies in the National Interest". https://www.industry.gov.au/publications/list-critical-technologies-national-interest

Australia. DSTG. (2022). Defence Science and Technology Group. "Socio-Technical Futures Analysis - EOI Opportunity". https://www.dst.defence.gov.au/news/2022/09/15/socio-technical-futures-analysis-eoi-opportunity

Australia. DSTG. (2024). Defence Science and Technology Group. "Accelerating Asymmetric Advantage – Delivering More, Together". Defence Innovation, Science and Technology Strategy". www.dst.defence.gov.au/strategy

Australia. DTA. (2024). Digital Transformation Agency. "Pilot AI assurance framework", November, https://www.digital.gov.au/policy/ai/pilot-ai-assurance-framework

Australia. Government (2020). "Australian Government response to the House of Representatives Standing Committee on Communications and the Arts: 'The Next Gen Future' Inquiry into the deployment, adoption and application of 5G in Australia". https://www.infrastructure.gov.au/sites/default/files/documents/australian-government-response-the-next-gen-future1.pdf

Australia. House of Representatives. (2014). Standing Committee on Social Policy and Legal Affairs. "Inquiry: Eyes in the sky: Inquiry into drones and the regulation of air safety and privacy", https://www.aph.gov.au/-/media/02_Parliamentary_Business/24_Committees/243_Reps_Committees/SPLA/Drones/fullreport.pdf

Australia. House of Representatives. (2020). Standing Committee on Communications and the Arts. “Next Gen: Inquiry into the Deployment, Adoption, and Application of 5G in Australia”, https://parlinfo.aph.gov.au/parlInfo/download/committees/reportrep/024373/toc_pdf/TheNextGenFuture.pdf
Australia. Infrastructure. (2024). Department of Infrastructure, Transport, Regional Development, Communications and the Arts. “Drone Privacy Guidelines”. https://www.drones.gov.au/sites/default/files/documents/Drone%20Privacy%20Guidelines.pdf
Australia. Office of National Intelligence. Australia. (n.d.). “Cyber and Critical Technology Intelligence Centre”, https://www.oni.gov.au/national-intelligence-community/cctic
Australia. Parliament (2024b). Joint Standing Committee on Foreign Affairs, Defence and Trade. “Inquiry into the Department of Defence Annual Report 2022–23”. https://parlinfo.aph.gov.au/parlInfo/download/committees/reportjnt/RB000427/toc_pdf/InquiryintotheDefenceAnnualReport2022%e2%80%9323.pdf
Australia. Parliament. (2015). Joint Committee on Treaties. “Report 151 Treaty tabled on 28 October 2014 Agreement between the Government of Australia and the Government of India on Cooperation in the Peaceful Uses of Nuclear Energy”. September. Canberra https://www.aph.gov.au//media/02_Parliamentary_Business/24_Committees/244_Joint_Committees/JSCT/2015/Report151/prelims.pdf
Australia. Parliament. (2017). Joint Committee on Intelligence and Security. “Review of the Telecommunications and Other Legislation Amendment Bill 2016”. https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/TSSRBill
Australia. Parliament. (2024a), Joint Standing Committee on Treaties. “Report 224: Agreement among the Government of Australia, the Government of the United Kingdom of Great Britain and Northern Ireland, and the Government of the United States of America for Cooperation Related to Naval Nuclear Propulsion”, November, https://parlinfo.aph.gov.au/parlInfo/download/committees/reportjnt/RB000533/toc_pdf/Report224.pdf
Australia. Parliament. (2024a). “Treaties Committee tables report on AUKUS agreement”, 27 November. https://www.aph.gov.au/About_Parliament/House_of_Representatives/About_the_House_News/Media_Releases/Treaties_Committee_tables_report_on_AUKUS_agreement
Australia. Parliament. (2025a). Parliamentary Joint Committee on Intelligence and Security. “Review of Administration and Expenditure No. 22 (2022–23) – Australian Intelligence Agencies”. https://parlinfo.aph.gov.au/parlInfo/download/committees/reportjnt/RB000434/toc_pdf/ReviewofAdministrationandExpenditure.pdf
Australia. Parliament. (2025b). Joint Committee on Public Accounts and Audit. “Report 510: Inquiry into the use and governance of artificial intelligence systems by public sector entities - 'Proceed with Caution'”. https://parlinfo.aph.gov.au/parlInfo/download/committees/reportjnt/RB000567/toc_pdf/Report510Inquiryintotheuseandgovernanceofartificialintelligencesystemsbypublicsectorentities-'ProceedwithCaution'.pdf
Australia. Productivity Commission. (2023). “5-year Productivity Inquiry: Australia’s data and digital dividend Inquiry report – volume 4”, https://www.pc.gov.au/inquiries/completed/productivity/report/productivity-volume4-data-digital-dividend.pdf
Australia. Senate. (1989). Senate Committee on Foreign Affairs, Defence and Trade. “Visits to Australia by nuclear powered or armed vessels: Contingency planning for the accidental release of ionizing radiation”. https://www.aph.gov.au/~/media/wopapub/senate/committee/fadt_ctte/completed_inquiries/pre1996/nuclear_warship_visits/report_pdf.ashx
Australia. Senate. (2012). “Constitutional Affairs Legislation Committee, Estimates”. 16 October 2012, https://parlinfo.”aph.gov.au/parlInfo/download/committees/estimate/0e2bb940-ccdc-4a20-b4e0-b3e6031771e8/toc_pdf/Legal%20and%20Constitutional%20Affairs%20Legislation%20Committee_2012_10_16_1457_Official.pdf;fileType=application%2Fpdf#search=%22committees/estimate/0e2bb940-ccdc-4a20-b4e0-b3e6031771e8/0000%22

Australia. Senate. (2015). Senate Foreign Affairs, Defence and Trade References Committee. "The potential use by the Australian Defence Force of unmanned air, maritime and land platforms", https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Foreign_Affairs_Defence_and_Trade/Defence_Unmanned_Platform/~/media/Committees/fadt_ctte/Defence_Unmanned_Platform/report.pdf

Australia. Senate. (2024a). "Select Committee on Adopting Artificial Intelligence: Final Report". November. https://parlinfo.aph.gov.au/parlInfo/download/committees/reportsen/RB000470/toc_pdf/SelectCommitteeonAdoptingArtificialIntelligence(AI).pdf

Australia. Senate. (2024b). Select Committee on Adopting Artificial Intelligence. "Interim Report" . October. https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Adopting_Artificial_Intelligence_AI/AdoptingAI/Interim_report

Australia. Senate. (2024c). Senate Finance and Public Administration Reference Committee *Supporting Sovereign Capability in the Australian Tech Sector*. https://parlinfo.aph.gov.au/parlInfo/download/committees/reportsen/RB000308/toc_pdf/Supportingthedevelopmentofsovereigncapabilityintheaustraliantechsector.pdf

Australia. Senate. (2024d). Senate References Committee on Rural and Regional Affairs and Transport. "Shutdown of the 3G mobile network: Interim Report", https://parlinfo.aph.gov.au/parlInfo/download/committees/reportsen/RB000474/toc_pdf/Shutdownofthe3GmobilenetworkInterimreport.pdf

Australian Trade and Investment Commission. (2023). "Australian Critical Technologies Prospectus", https://international.austrade.gov.au/en/do-business-with-australia/sectors/technology/australian-critical-technologies-prospectus

Bachhawat, A., Cave, D., Kang, J., Rajagopalan, R. P., & Ray, T. (2020). "Critical technologies and the Indo-Pacific". *Australian Strategic Policy Institute,* https://www.aspi.org.au/report/critical-technologies-and-indo-pacific-new-india-australia-partnership

Banta, D. (2009). "What is technology assessment?" *International Journal of Technology Assessment in Health Care*, 25(S1), pp. 7-9, https://doi.org/10.1017/S0266462309090333

Barik, S. (2024). "After criticism, govt clarifies: AI startups don't need IT Ministry approval". *The Indian Express*. 5 March. https://indianexpress.com/article/business/genai-startups-dont-need-to-seek-govt-nod-before-launch-rajeev-chandrasekhar-9194613/

Barnes, P. (2018) "Avoiding surprises: technology assessment and foresight", The Strategist, 6 December. https://www.aspistrategist.org.au/avoiding-surprises-technology-assessment-and-foresight/

BBC News. (2012). "China's Huawei barred from Australia broadband deal", 26 March, https://www.bbc.com/news/business-17509201

Bimber, B. and Popper, S. W. (1994). "*What is a Critical Technology?"* RAND Institute, https://www.rand.org/pubs/drafts/DRU605.html

Boardman, A. E., Greenberg, D. H., Vining, A. R., & Weimer, D. L. (2017). *Cost-benefit Analysis: Concepts and Practice*, Cambridge, Cambridge University Press

Bradfield, R., Wright, G., Burt, G., Cairns, G., & van der Heijden, K. (2005). "The origins and evolution of scenario planning". *Futures*, 37(6), pp. 795-812.

Brodtmann, G., Caples, A., Cave, D., & Keast, J. (2023). "What Do Australia's Parliamentarians Think about Cybersecurity and Critical Technology?" *Australian Strategic Policy Institute,* https://www.aspi.org.au/report/what-do-australias-parliamentarians-think-about-cybersecurity-and-critical-technology

Capri, A. (2022). "CHIPS on the table: US doubles down on techno-nationalism", *Hinrich Foundation*, https://www.hinrichfoundation.com/research/article/tech/chips-us-techno-nationalism

Chaudhuri, R. and Bhandari, K. (2024). "The U.S.–India Initiative on Critical and Emerging Technology (iCET) from 2022 to 2025: Assessment, Learnings, and the Way Forward', *Carnegie Endowment for International Peace*, Washington D.C. https://carnegieendowment.org/research/2024/10/the-us-india-initiative-on-critical-and-emerging-technology-icet-from-2022-to-2025-assessment-learnings-and-the-way-forward

Chen Y. and Wu S. (2024). "Regulating unmanned aircraft systems in Antarctica: challenges and collaborative solutions". *Front. Mar. Sci.*, 11, art. 1486894, https://doi.org/10.3389/fmars.2024.1486894

Chmielewski, P. (2025). "Vulnerable Agents and Sustainable Security", *IEEE Transactions on Technology and Society*, 6(1), pp. 102-111, https://doi.org/10.1109/TTS.2024.3465376

Clarke, R. (2025). "A Brief Overview of Technology/ical {Impact} Assessment", https://roger-clarke.com/EC/TIAN.html#App2

Clarke, R. and Michael, K. (2024). "Multi-Stakeholder Risk Assessment of Socio-Technical Interventions". *ACIS 2024 Proceedings*. https://aisel.aisnet.org/acis2024/1

Clarke, R. and Moses, L. B. (2014). The Regulation of Civilian Drones' Impacts on Public Safety. *Computer Law & Security Review*, 30, 263-285. https://doi.org/10.1016/j.clsr.2014.03.007

CUTS. (n.d.) "Ethical 6G – Identifying Elements of Ethical Framework for 6G and Creating Opportunities for India and Australia". *CUTS*, https://cuts-ccier.org/ethical-6g-identifying-elements-of-ethical-framework-for-6g-and-creating-opportunities-for-india-and-australia/

Davidson, M. A. (2005). "A matter of degrees". *Security Management,* 49(12), pp. 72-99.

Decker, M., Ladikas, M. (2004). "Technology Assessment in Europe; between Method and Impact — The TAMI Project" in Decker, M., Ladikas, M., Stephan, S., Wütscher, F. (eds) *Bridges between Science, Society and Policy*, Wissenschaftsethik und Technikfolgenbeurteilung, vol 22. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-06171-8_1

DigitalDefynd. (2024) "10 examples of AI being used in Defense Sector". https://digitaldefynd.com/IQ/ai-use-in-defense-sector/

Australia. DTA. (2024). Digital Transformation Agency. "Pilot AI assurance framework", November, https://www.digital.gov.au/policy/ai/pilot-ai-assurance-framework

Dortmans, P., Nicholson, J., Yeung, J., Black, J., Dewaele, L., and Knack A. (2022). "Prioritising Critical Technologies of National Interest in Australia: Developing an Analytical Approach", *Rand Australia*, https://www.rand.org/pubs/research_reports/RRA1534-1.html

Drezner, D. W. (2024). "How Everything Became National Security". *Foreign Affairs*, 12 August. https://www.foreignaffairs.com/united-states/how-everything-became-national-security-drezner

Dunlap, C. (2021) "If everything is a 'national security' priority, nothing will be". 21 May. https://sites.duke.edu/lawfire/2021/05/12/if-everything-is-a-national-security-priority-nothing-will-be/

European Union Aviation Safety Agency. (2021). "Boeing 737 MAX Return to Service Report Overview of the Technical Investigation Activities Performed by EASA". https://www.easa.europa.eu/sites/default/files/dfu/B737_Max_Return_to_Service_Report.pdf

Federal Register of Legislation. (2024). "Migration (Critical Technology – Kinds of Technology) Specification (LIN 24/010)", https://www.legislation.gov.au/F2024L00182/asmade/text

Ferrey, S. (2016). "Presidential Executive Action: Unilaterally Changing the World's Critical Technology and Infrastructure". *Drake Law Review,* 64, pp. 43-110.

Fischer, R. J., & Green, G. (2004). *Introduction to Security*, Boston, Butterworth-Heinemann.

Fitch, A., & Woo, S. (2020). "The US vs. China: Who Is Winning the Key Technology Battles?" *Wall Street Journal*, 12 April.

Gill, S. S., Kumar, A., Singh, H., Singh, M., Kaur, K., Usman, M., Buyya, R. (2022). "Quantum computing: A taxonomy, systematic review and future directions," *Software: Practice and Experience,* 52(1), pp. 66-114.

Giovanardi, M. (2024). "AI for peace: mitigating the risks and enhancing opportunities, *Data & Policy*, 6, e41. Cambridge University Press. https://www.cambridge.org/core/services/aop-cambridge-core/content/view/797BCCFF182A0367F2A99FC5FB064150/S2632324924000373a.pdf/ai-for-peace-mitigating-the-risks-and-enhancing-opportunities.pdf

Goswami A, Panicker R, Colonel Das KPM. (2025). "Securing the Electronic Hardware Supply Chain: A Cost-Benefit Analysis Framework", Takshashila Discussion Document – 2025-07, The Takshashila Institution.

https://static1.squarespace.com/static/618a55c4cb03246776b68559/t/67ecdd9fb5f9ed1e6f52dcaa/1743576490477/Takshashila+Discussion+Document+-+HSCS.pdf
Grunwald, A. (2009) "Technology Assessment: Concepts and Methods" in Meijers, A. (ed) *Handbook of the Philosophy of Science*, pp. 103-1146. https://doi.org/10.1016/B978-0-444-51667-1.50044-6. https://www.sciencedirect.com/science/article/pii/B9780444516671500446
Gupta K. (2021) "Member Consultation-MoCA releases Draft Drone Rules, 2021", NASSCOM. https://community.nasscom.in/communities/policy-advocacy/member-consultation-moca-releases-draft-drone-rules-2021
Hagemann, Ryan and Huddleston, Jennifer and Thierer, Adam D. (2018). "Soft Law for Hard Problems: The Governance of Emerging Technologies in an Uncertain Future". *Colorado Technology Law Journal*, Available at SSRN: https://ssrn.com/abstract=3118539
Hardy, P. (2025) "Drones for emergency services: a whole-of-government approach to crisis prevention, response and recovery", *Australian Journal of Emergency Management*, January. https://knowledge.aidr.org.au/resources/ajem-january-2025-drones-for-emergency-services-a-whole-of-government-approach-to-crisis-prevention-response-and-recovery/
Heim, L. (2025). "Can export controls create a U.S.-led global artificial intelligence ecosystem?" *RAND*, 14 January. https://www.rand.org/pubs/perspectives/PEA3776-1.html
Howie, E. (2025) "Australia needs to be transparent on armed drones", Human Rights Law Centre. https://www.hrlc.org.au/updates/australia-needs-to-be-transparent-on-armed-drones/
HTAIn. (2025). "Health Technology Assessment in India- Attached Office Under Department of Health Research", https://dhr.gov.in/health-technology-assessment-india-htain
IAEA. (2015), International Atomic Energy Agency. "IAEA Mission Concludes Peer Review of India's Nuclear Regulatory Framework", 27 March. https://www.iaea.org/newscenter/pressreleases/iaea-mission-concludes-peer-review-indias-nuclear-regulatory-framework
IAEA. (2025). International Atomic Energy Agency. "Nuclear safety conventions". https://www.iaea.org/topics/nuclear-safety-conventions
ICAO. (2014). International Civil Aviation Or5ganisatioon. "Introduction to Model UAS Regulations and Advisory Circulars". https://www.icao.int/safety/UA/Pages/ICAO-Model-UAS-Regulations.aspx
ICAO (2022). International Civil Aviation Organisation. "Summary of fuels-related information from the ICAO Long-term Aspirational goal (LTAG) Analyses". https://www.icao.int/environmental-protection/LTAG/Documents/Summary%20of%20LTAG%20information%20on%20fuels.pdf
ICMR. (2023). Indian Council of Medical Research. "Ethical guidelines for application of Artificial Intelligence in Biomedical Research and Healthcare".
IIT. (2023). Indian Institute of Technology Madras. "IIT Madras establishes Centre for Responsible AI". https://www.iitm.ac.in/happenings/press-releases-and-coverages/iit-madras-establishes-centre-responsible-ai
India. (2024) Ministry of Space. "India Space Situational Awareness Report 2023". https://www.drishtiias.com/pdf/1747458134.pdf
India. (2024). Ministry of Science and Technology. "National Quantum Mission". https://dst.gov.in/national-quantum-mission-nqm
India. CEA. (2024). Central Electricity Authority. https://cea.nic.in/wp-content/uploads/regulations_cpt/2024/08/Draft_CEA_Cyber_Security_in_Power_Sector_Regulations_2024.pdf
India. DAE. (2022) Department of Atomic Energy. "Cyber Security Breach in Nuclear Plants", Press Release, 23 MAR 2022. https://pib.gov.in/PressReleasePage.aspx?PRID=1808677
India. Lok Sabha. (2023). "Lok Sabha Unstarred Question No. 4460", https://sansad.in/getFile/loksabhaquestions/annex/1711/AU4460.pdf?source=pqals
India. Lok Sabha. (2024). Bulletin-Part II. (General Information relating to Parliamentary and other matters) Nos. 856 - 859, Tuesday, October 8, 2024, Asvina 16, 1946,(Saka), https://www.medianama.com/wp-content/uploads/2024/10/bull2mk_2024_08-10-24.pdf

India. MEA. (2020a). Ministry of External Affairs. "India Framework Agreement on Cyber and Cyber-enabled Critical Technology Cooperation between the Republic of India and the Government of Australia". https://www.mea.gov.in/Portal/LegalTreatiesDoc/AU20B3708.pdf
India. MEA. (2020b). Ministry of External Affairs. "2020-2025 Plan of Action under the Framework Agreement on Cyber Cooperation between the Republic of India and the Government of Australia", https://www.mea.gov.in/Portal/LegalTreatiesDoc/AU20B3708.pdf [pp. 5-7]
India. MEA (2021). Ministry of External Affairs. Treaties Database. "Agreement between the European Atomic Energy Community and the Government of The Republic of India for Research and Development Cooperation in the Field of the Peaceful Uses of Nuclear Energy. https://www.mea.gov.in/Portal/LegalTreatiesDoc/020I3818-1.pdf
India. MeitY. (2024a). Ministry of Electronics & IT. "Cabinet Approves Over Rs 10,300 Crore for IndiaAI Mission, will Empower AI Startups and Expand Compute Infrastructure Access". https://pib.gov.in/PressReleasePage.aspx?PRID=2012375
India. MeitY. (2024b). Ministry of Electronics & IT. "UNESCO and MeitY organise National Stakeholder Workshop on Ethics of AI". https://pib.gov.in/PressReleaseIframePage.aspx?PRID=2022930
India. Ministry of Finance. (2020). "Restrictions on Public Procurement from Certain Countries. 23 July. https://pib.gov.in/PressReleasePage.aspx?PRID=1640778
India. NSC. (2020). National Security Council Secretariat. "National Security Directive on Telecommunication Sector". https://dot.gov.in/sites/default/files/Brief%20on%20launch%20of%20Trusted%20Telecom%20Portal-1.pdf
India. NITI Aayog. (2018). National Institution for Transforming India. "National Strategy for Artificial Intelligence #AIForAll". https://www.niti.gov.in/sites/default/files/2023-03/National-Strategy-for-Artificial-Intelligence.pdf
India NITI Aayog. (2021). National Institution for Transforming India. "Operationalising Principles". https://indiaai.gov.in/research-reports/responsible-ai-part-2-operationalizing-principles-for-responsible-ai
India. NITI Aayog. (2021). National Institution for Transforming India. "Responsible AI Approach Document for India Part 1 – Principles for Responsible AI". https://www.niti.gov.in/sites/default/files/2021-02/Responsible-AI-22022021.pdf
India. NITI Aayog. (2022). National Institution for Transforming India. "A use case approach on Facial Recognition Technology". https://www.niti.gov.in/sites/default/files/2022-11/Ai_for_All_2022_02112022_0.pdf
India. NITI Aayog. (2025) National Institution for Transforming India. "Quantum Computing: National Security Implications & Strategic Preparedness". *Frontier Tech Hub Quarterly Frontier Insights*. https://www.niti.gov.in/sites/default/files/2025-03/Future-Front-Quarterly-Frontier-Tech-Insights-March-2025.pdf
India. PIB. (2022). Press and Information Bureau. "Cyber Security Breach in Nuclear Plants". 23 March. https://www.pib.gov.in/PressReleasePage.aspx?PRID=1808677
India. Rajya Sabha. (2022). Unstarred Question No. 165 (Winter Session 2022) Government of India Department of Atomic Energy Rajya Sabha Unstarred Question no. 162 to be answered on 08.12.2022 "Cyber threats to nuclear plants", https://cdnbbsr.s3waas.gov.in/s35b8e4fd39d9786228649a8a8bec4e008/uploads/2023/02/2023020810-3.pdf
India. RBI. (2023). Reserve Bank of India. "Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices". https://www.rbi.org.in/scripts/Notification-User.aspx?Id=12562&Mode=0
India. RBI. (2024). Reserve Bank of India. "Press release on 'Framework for Responsible and Ethical Enablement (FREE) of Artificial Intelligence (AI) in the Financial Sector'". https://www.rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=59377
IndiaAI. (2025). "Report on AI governance guidelines development". https://indiaai.gov.in/article/report-on-ai-governance-guidelines-development

Indian Council of World Affairs. (2024). “Emerging Technologies and Indian Diplomacy: Artificial Intelligence, Semiconductors, Nanotechnology”, *ICWA*, https://www.icwa.in/showlink.php?lang=1&level=3&ls_id=10387&lid=6621

Inside FPV Social. (2025a) “Drone Laws in 2025: What Every Drone Operator Needs to Know”. https://insidefpv.com/blogs/blogs/drone-laws-in-2025-what-every-drone-operator-needs-to-know

Inside FPV Social (2025b) “Are Drones a Silent Danger to Nuclear Power Plants?”. https://insidefpv.com/blogs/blogs/are-drones-a-silent-danger-to-nuclear-power-plants?

Jeník, I. and Duff, S. (2020). *How to build a regulatory sandbox: A practical guide for policy makers*. Technical Guide. Washington, D.C., CGAP. https://documents.worldbank.org/en/publication/documents-reports/documentdetail/126281625136122935/how-to-build-a-regulatory-sandbox-a-practical-guide-for-policy-makers

Jha-Thakur, U. and Khosravi, F. (2021) “Beyond 25 years of EIA in India: Retrospection and way forward”, *Environmental Impact Assessment Review*, Volume 87. https://doi.org/10.1016/j.eiar.2020.106533. https://www.sciencedirect.com/science/article/pii/S0195925520308118

Jones, B. (1983). “Science And Technology Statement 1982-83”, May, https://www.industry.gov.au/sites/default/files/1982-83-science-technology-statement.pdf

Kiran, A.H., Oudshoorn, N., and Verbeek, P-P. (2015). "Beyond checklists: toward an ethical-constructive technology assessment." *Journal of Responsible Innovation*, 2(1), pp. 5-19. https://www.tandfonline.com/doi/full/10.1080/23299460.2014.992769?scroll=top&needAccess=true

Krause, K. (2004). “The Key to a Powerful Agenda, if Properly Delimited”. *Security Dialogue,* 35(3), pp. 367-368.

Landeta, J. (2006). “Current validity of the Delphi method in social sciences”. *Technological Forecasting and Social Change*, 73(5), pp. 467-482.

Luo, Y., and Van Assche, A. (2023). “The rise of techno-geopolitical uncertainty: Implications of the United States CHIPS and Science Act.” *Journal of International Business Studies,* 54(8), pp. 1423-1440.

Mallick, P. K. (2019). “Cyber Attack on Kudankulam Nuclear Power Plant: A Wake-Up Call”. New Delhi, Vivekananda International Foundation, https://www.vifindia.org/sites/default/files/cyber-attack-on-kudankulam-nuclear-power-plant.pdf

Mankins, J. C. (2009). “Technology readiness assessments: A retrospective”. *Acta Astronautica*, 65(9–10), pp. 1216–1223, https://doi.org/10.1016/j.actaastro.2009.03.058

Michael, K. (2021). "DARPA's ADAPTER Program: Applying the ELSI Approach to a Semi-Autonomous Complex Socio-Technical System," *2021 IEEE Conference on Norbert Wiener in the 21st Century (21CW)*, Chennai, India, pp. 1-10, doi: 10.1109/21CW48944.2021.9532581

Meerts, C. (2019) “Security: Concepts and Definitions”, Shapiro, L., Maras, MH. (eds) *Encyclopedia of Security and Emergency Management*. Springer, Cham. DOI:10.1007/978-3-319-69891-5_94-2

Michael, K., Abbas, R., Pitt, J., Vogel, K. and Zafeirakopoulos, M., "Securitization for Sustainability of People and Place", *IEEE Technology and Society Magazine*, 42(2), pp. 22-28, June 2023, https://doi.org/10.1109/MTS.2023.3283829

Michael, K., Vogel K. M., Pitt, J. and Zafeirakopoulos, M. (2025). "Artificial Intelligence in Cybersecurity: A Socio-Technical Framing," *IEEE Transactions on Technology and Society*, 6(1), pp. 15-30, March 2025, https://doi.org/10.1109/TTS.2024.3460740

Miller, C. (2022). *Chip War: The Fight for the World’s Most Critical Technology*, New York, Simon and Schuster.

Mohanty, A., and Sahu, S. (2024). “India’s advance on AI regulation”. Carnegie Endowment for International Peace. https://carnegieendowment.org/research/2024/11/indias-advance-on-ai-regulation

Moral-Muñoz, J. A., Herrera-Viedma, E., Santisteban-Espejo, A., & Cobo, M. J. (2020). “Software tools for conducting bibliometric analysis in science: An up-to-date review”. *Profesional De La información*, 29(1), https://doi.org/10.3145/epi.2020.ene.03

Naik, S., Kumar, A., Saxena, A., Todi, S. (2024). “Assessing the Global and Local Landscape of ‘Critical Technologies’”, Takshashila Institution.

https://static1.squarespace.com/static/618a55c4cb03246776b68559/t/65be46229bd37e7b4bf30dd6/1706968617851/Critical+Technologies-Takshashila+IC+Compendium+January+2024-V1.0.pdf

NASSCOM. (2024). National Association of Software and Service Companies. "The Developer's Playbook for Responsible AI in India", https://nasscom.in/ai/pdf/the-developer's-playbook-for-responsible-ai-in-india.pdf

National Academies (2017). "Human-genome-editing-science-ethics-and-governance". https://nap.nationalacademies.org/catalog/24623/human-genome-editing-science-ethics-and-governance

NNCTA. (2023). National Network for Critical Technology Assessment. "Securing America's Future: A Framework for Critical Technology Assessment" https://nncta.org/_files/documents/nncta-final-report.pdf

NSCAI. (2021) National Security Commission on Artificial Intelligence. "Final Report: National Security Commission on Artificial Intelligence", https://assets.foleon.com/eu-central-1/de-uploads-7e3kk3/48187/nscai_full_report_digital.04d6b124173c.pdf

Norton Rose Fullbright (2016) "Rise of the Drones: Opportunity and liability for Australian businesses". https://www.nortonrosefulbright.com/en-bi/knowledge/publications/7b7067d8/rise-of-the-drones-opportunity-and-liability-for-australian-businesses

OECD. (n.d.). Organisation for Economic Cooperation and Development. "Emerging Technologies", https://www.oecd.org/en/topics/emerging-technologies.html

OECD. (2024), Organisation for Economic Cooperation and Development. "Principles for Trustworthy AI". https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449

Palm, E., and Hansson, S-O. (2006). "The case for ethical technology assessment (eTA)." *Technological Forecasting & Social Change*, 73, pp. 543–558

Patil, S., and Arora, R. (2023). "Countering Hostile Drone Activity on the India Pakistan Border." Issue Brief No. 640, *Observer Research Foundation*, May 2023. https://www.orfonline.org/research/countering-hostile-drone-activity-on-the-india-pakistan-border

Postman, N. (1993). *Technopoly: The surrender of culture to technology*. Vintage.

Rajagopalan. R, Patil, S., Ajaykumar, S., and Tripathi, P. (2024). "Reducing India's Risks To Nuclear Terrorism", *Observer Research Foundation*, 2024, https://www.orfonline.org/public/uploads/posts/pdf/20240827103424.pdf

Rajagopolan, R., Krishna, R. Singh, L., Biswas, A. (2016) "Nuclear Security in India", second edition. Observer Research Foundation. https://www.orfonline.org/public/uploads/posts/pdf/20230411113546.pdf

Rajagopalan, R.P., Krishna, R. (2019). "India's Drone Policy: Domestic and Global Imperatives". ICAO Scientific Review: Analytics and Management Research, 1, 53-68. http://isr.icao.int/amr/Volume01/v1p053-068Rajagopalan5144.pdf

Reddy, B. and Naik, S. (2025). "A Framework for Governing Emerging Technologies", Takshashila Discussion, Document No. 2025-02, January 2025, The Takshashila Institution. https://takshashila.org.in/research/a-framework-for-governing-emerging-technologies

Reuters. (2019). "Australian Government reportedly advised India to Ban Huawei from the 5G network". *South China Morning Post*, 10 September. https://www.scmp.com/news/asia/australasia/article/3026452/australian-government-reportedly-advised-india-ban-huawei-5g

Rotolo, D., Hicks, D. and Martin, B.R. (2015). "What is an emerging technology?", *Research Policy*, 44(10), pp. 1827-1843, https://doi.org/10.1016/j.respol.2015.06.006

Saarnisaari, H., Dixit, S., Alouini, M.-S., Chaoub, A., Giordani, M., Kliks, A., Matinmikko-Blue, M., & Zhang, N. (Eds.). (2020). *6G White Paper on Connectivity for Remote Areas*. 6G Research Visions, No. 5. University of Oulu, http://urn.fi/urn:isbn:9789526226750

Sahni, S. (2024). "The Inception and Evolution of India's Nuclear Program", GeoStrata, https://www.thegeostrata.com/post/the-evolution-of-india-s-nuclear-program

Saikhu, A. (2024). "Cyber Escalation and Nuclear Stability: Assessing the Role of Cyber Warfare in India-Pakistan Deterrence". *Defence Journal*, 10 June.

Sanyal, S., Sharma, P., and Dudani, C. (2024). "A Complex Adaptive System Framework to Regulate Artificial Intelligence". *Economic Advisory Council to the PM* EAC-PM/WP/26/2024, https://eacpm.gov.in/wp-content/uploads/2024/01/EACPM_AI_WP-1.pdf

Sarangi, S. (2019) "National Initiatives on Artificial Intelligence in Defence", United Service Institution, https://www.usiofindia.org/strategic-perspective/national-initiatives-on-artificial-intelligence-in-defence.html

Senge, P. M. (1990). *The Fifth Discipline: The Art & Practice of the Learning Organization*, Doubleday/Currency.

SBS News. (2018). "Intelligence boss defends 5G security step", *SBS*, 7 December. https://www.sbs.com.au/news/article/intelligence-boss-defends-5g-security-step/t41arcxjw

Schatzberg, E. (2018). *Technology: critical history of a concept.* Chicago, University of Chicago Press.

Schmid, Jon, Chad J. R. Ohlandt, and Cochran, S. (2024). "Net Technical Assessment: A Methodology for Assessing Military Technology Competition", Santa Monica, CA, RAND Corporation. https://www.rand.org/pubs/research_reports/RRA1350-1.html

SIPRI. (2025). Stockholm International Peace Research Institute. "Artificial Intelligence, Non-proliferation and Disarmament: A Compendium on the State of the Art". EU Non-Proliferation and Disarmament Papers. https://www.sipri.org/publications/2025/eu-non-proliferation-and-disarmament-papers/artificial-intelligence-non-proliferation-and-disarmament-compendium-state-art

Shashidhar K. J. (2023). "Regulatory Sandboxes: Decoding India's attempt to Regulate Fintech Disruption", Observer Research Foundation (ORF). https://www.orfonline.org/research/regulatory-sandboxes-decoding-indias-attempt-to-regulate-fintech-disruption-66427

Shubayr, N. (2024). "Nuclear security measures: A review of selected emerging technologies and strategies", *Journal of Radiation Research and Applied Sciences*, 17(1), https://doi.org/10.1016/j.jrras.2023.100814

Srinivas, Ravi Krishna and van Est, Rinie (2023). "Technology Assessment in Developing Countries: The Case of India — Examples of Governmental and Informal TA" in *Technology Assessment in a Globalized World*, DOI:10.1007/978-3-031-10617-0_6

Statesman. (2024). "Indian Army partners with BEL to establish an advanced AI hub in Bengaluru", https://www.thestatesman.com/india/indian-army-partners-with-bel-to-establish-advanced-ai-hub-in-bengaluru-1503377185.html

Mohan, P. (2021). "Can India Address the Growing Cybersecurity Challenges in the Nuclear Domain?" *Stimson Center*, https://www.stimson.org/2021/can-india-address-the-growing-cybersecurity-challenges-in-the-nuclear-domain/

Suchman, L. (2021). "Six Unexamined Premises Regarding Artificial Intelligence and National Security", *AI-Now Institute*, 31 March. https://ainowinstitute.org/publication/six-unexamined-premises-regarding-artificial-intelligence-and-national-security

Sukumar, A. (2019). Midnight's Machines - A Political History of Technology in India. Penguin Random House, India.

Todi, S. (2024). "What should India's critical technology policy look like?", Takshashila Institution Discussion Document 2024-09. https://static1.squarespace.com/static/618a55c4cb03246776b68559/t/6669e9ab6ad1b859a8b4ae6b/1718217137121/CET+Policy+Framework.pdf

Tuvdendarjaa, Munkh-Orgil. (2025). "Artificial Intelligence in Contemporary Peacekeeping Operations". Daniel K. Inouye Asia-Pacific Center for Security Studies (DKIAPCSS). https://dkiapcss.edu/nexus_articles/artificial-intelligence-in-contemporary-peacekeeping-operations/

Uren, T. and Cave, D. (2018). "Why Australia banned Huawei from its 5G telecoms network." *Australian Strategic Policy Institute*. 30 August, https://www.aspi.org.au/opinion/why-australia-banned-huawei-its-5g-telecoms-network

UNCTAD. (2024). United Nations Conference on Trade and Development. "Technology Assessment in Developing Countries: An Updated Proposed Methodology". https://unctad.org/system/files/official-document/tcsdtlinf2024d6_en.pdf

UNDP. (2019). United Nations Development Program. “25th Anniversary of the Human Security concept”. https://www.undp.org/speeches/25th-anniversary-human-security-concept
United Kingdom. (2020b). “Huawei to be removed from UK 5G networks by 2027”, 14 July. https://www.gov.uk/government/news/huawei-to-be-removed-from-uk-5g-networks-by-2027
United Kingdom. (2020a). “Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board Annual Report.” (6th Report) https://assets.publishing.service.gov.uk/media/5f75bc438fa8f54e8fb2d1e2/Huawei_Cyber_Security_Evaluation_Centre__HCSEC__Oversight_Board-_annual_report_2020.pdf
United Kingdom. (2020b). “Huawei to be removed from UK 5G networks by 2027”, 14 July. https://www.gov.uk/government/news/huawei-to-be-removed-from-uk-5g-networks-by-2027
United Nations. (1999) “Declaration and Programme of Action on a Culture of Peace”, UN. Doc. A/RES/53/243, available at http://un-documents.net/a53r243.htm
United States. (2021). White House. “Quad Principles on Technology Design, Development, Governance, and Use”, The White House. https://www.whitehouse.gov/briefing-room/statements-releases/2021/09/24/quad-principles-on-technology-design-development-governance-and-use/
United States. (2024), White House. “Joint Fact Sheet: The United States and India Continue to Chart an Ambitious Course for the Initiative on Critical and Emerging Technology”, 17 June. https://biden-whitehouse.archives.gov/briefing-room/statements-releases/2024/06/17/joint-fact-sheet-the-united-states-and-india-continue-to-chart-an-ambitious-course-for-the-initiative-on-critical-and-emerging-technology/
United States. NASA. (2025). National Aeronautics and Space Administration. “Advanced Air Mobility Mission”. Web-page https://www.nasa.gov/mission/aam/
United States. (2025). White House. “America First investment policy”, 21 February. https://www.whitehouse.gov/presidential-actions/2025/02/america-first-investment-policy/
United States. Congress. (1976). “Technology Assessment Activities in the Industrial. Academic, and Governmental Communities”, 8 June. Technology Assessment Board. Office of Technology Assessment. https://www.princeton.edu/~ota/disk3/1976/7622/7622.PDF
United States. (1972). Public Law 92-484-OCT. 13, 1972. 7970803. https://www.congress.gov/92/statute/STATUTE-86/STATUTE-86-Pg797.pdf
United States. (1998). Public Law 105–271—Oct. 19, 1998. Year 2000 Information and Readiness Disclosure Act. https://www.govinfo.gov/content/pkg/PLAW-105publ271/pdf/PLAW-105publ271.pdf
UNODA (n.d.) United Nations Office of Disarmament Affairs. “Global Issues: Disarmament”. https://www.un.org/en/global-issues/disarmament
Noetel, M., Saeri, A., Graham, J. (2024). “80% of Australians think AI risk is a global priority. The government needs to step up”, University of Queensland, Research. 11 March. https://www.uq.edu.au/research/article/2024/03/80-australians-think-ai-risk-global-priority-government-needs-step
UTM Policy Framework. (2021). National Unmanned Aircraft System Traffic Management (UTM) Policy Framework, 24-October-2021, https://digitalsky.dgca.gov.in/assets/files/National-UTM-Policy-Framework-2021-24-Oct-2021.pdf
Vietti, F. & Scribner, T. (2013). “Human Insecurity: Understanding International Migration from a Human Security Perspective”, *Journal on Migration and Human Security,* 1(1), https://doi.org/10.1016/j.jrras.2023.100814
Walker-Munro, B. (2025). “Defining National Security: Still a Non-Justiciable Problem?” *Public Law Review*, Public law review, Vol.36(1), pp.58-75.
Weingart, P. (1991). “Large technical systems, real life experiments, and the legitimation trap of technology assessment: The contribution of science and technology to constituting risk perception”, in T. R. LaPorte (ed.), *Social responses to large technical systems: Control or anticipation*, Kluwer. NATO ASI Series, vol 58. Springer, Dordrecht. https://doi.org/10.1007/978-94-011-3400-2_1
Wiedemann, M., Vij, A., Banerjee, R., O’Connor, A., Soetanto, D., Ardeshiri, A., Wittwer, G., Sheard, N.(2023) “Validating the benefits of increased drone uptake for Australia: geographic, demographic and social insights”. https://apo.org.au/sites/default/files/resource-files/2023-04/apo-nid322458.pdf

Williams, P. D. (2012) “Security Studies: An Introduction”, in Paul D. Williams (Ed.), *Security Studies*: *An Introduction*, Abingdon: Routledge, pp. 1-12.

Withers, G., West, E., Buchanan, L., Clements, D., and Austin, G. (2019) “Social Science Research and Intelligence in Australia”, Academy of the Social Sciences in Australia. https://socialsciences.org.au/publications/social-science-research-intelligence-in-australia/

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, N. (2024). "Assessing AI Technologies for LEA Use: The ALIGNER Methodology". In *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-9781035310678.html

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, 20, 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. In Klude 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 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.

Inquiries

karthik@klude.in

greg.austin@socialcyber.co

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