Negotiating technical standards for artificial intelligence

A techdiplomacy playbook for policy-makers and technologists in the Indo-Pacific

BART HOGEVEEN
ARINDRAJIT BASU
ISHA SURI
BAANI GREWAL

JUNE 2024

Policy Brief

ASPI
AUSTRALIAN STRATEGIC POLICY INSTITUTE

Centre for Internet & Society

About the authors

Bart Hogeveen is Deputy Director, Cyber, Technology and Security at ASPI.
Arindrajit Basu is a Non-Resident Research Fellow at the Centre for Internet and Society (CIS), India, and a PhD candidate at Leiden University, the Netherlands.
Isha Suri is a Research Lead at the Centre for Internet and Society, India.
Baani Grewal is a former analyst at ASPI.

Acknowledgements

ASPI acknowledges the Ngunnawal and Ngambri peoples, who are the traditional owners and custodians of the land upon which this work was prepared, and their continuing connection to land, waters and community. We pay our respects to their cultures, country and elders past, present and emerging.

The authors would like to thank Manoj Harjani, Gurshabad Grover, Geoff Clarke, Alexandra Caples, Danielle Cave, Mercedes Page, Jacinta Keast, Bronte Munro, Yuta Kimura, Yvonne Lau, Antara Vats, Huon Curtis, Shweta Mohandas, Abhishek Raj and other colleagues at ASPI and CIS for their valuable feedback. We would also like to thank Peter Cihon for his valuable insights.

We are grateful to counterparts at the Australian government's Department of Foreign Affairs and Trade and Department of Industry, Science and Resources, Standards Australia and the Bureau of Indian Standards for their feedback and suggestions. We also like to thank the Joint Secretary for New, Emerging and Sensitive Technologies at the Indian Ministry of External Affairs for their keynote address at a launch event in Delhi in October 2023.

About ASPI

The Australian Strategic Policy Institute was formed in 2001 as an independent, non-partisan think tank. Its core aim is to provide the Australian Government with fresh ideas on Australia's defence, security and strategic policy choices. ASPI is responsible for informing the public on a range of strategic issues, generating new thinking for government and harnessing strategic thinking internationally. ASPI's sources of funding are identified in our Annual Report, online at www.aspi.org.au and in the acknowledgements section of individual publications. ASPI remains independent in the content of the research and in all editorial judgements. It is incorporated as a company, and is governed by a Council with broad membership. ASPI's core values are collegiality, originality & innovation, quality & excellence and independence.

ASPI's publications—including this paper—are not intended in any way to express or reflect the views of the Australian Government. The opinions and recommendations in this paper are published by ASPI to promote public debate and understanding of strategic and defence issues. They reflect the personal views of the author(s) and should not be seen as representing the formal position of ASPI on any particular issue.

ASPI Cyber, Technology and Security

ASPI's Cyber, Technology and Security (CTS) analysts aim to inform and influence policy debates in the Indo-Pacific through original, rigorous and data-driven research. CTS remains a leading voice in global debates on cyber, emerging and critical technologies, foreign interference and issues related to information operations and disinformation. CTS has a growing mixture of expertise and skills with teams of researchers who concentrate on policy, technical analysis, information operations and disinformation, critical and emerging technologies, cyber capacity building and Internet safety, satellite analysis, surveillance and China-related issues. To develop capability in Australia and across the Indo-Pacific region, CTS has a capacity building team that conducts workshops, training programs and large-scale exercises for the public, private and civil society sectors. Current projects are focusing on capacity building in Southeast Asia and the Pacific Islands region, across a wide range of topics. CTS enriches regional debate by collaborating with civil society groups from around the world and by bringing leading global experts to Australia through our international fellowship program. We thank all of those who support and contribute to CTS with their time, intellect and passion for the topics we work on. If you would like to support the work of the CTS, contact: ctspartnerships@aspi.org.au.

Funding

Funding for this report was provided by the Australian Department of Foreign Affairs and Trade.

Cover artwork: everything.design, online.

Negotiating technical standards for artificial intelligence

A techdiplomacy playbook for policy-makers and technologists in the Indo-Pacific

BART HOGEVEEN
ARINDRAJIT BASU
ISHA SURI
BAANI GREWAL

JUNE 2024

Policy Brief

ASPI
AUSTRALIAN STRATEGIC POLICY INSTITUTE

Centre for Internet & Society

Website

This report is accompanied by a web page that can be accessed via: **www.aspi.org.au/techdiplomacy**

About the Centre for Internet and Society

The Centre for Internet and Society is a non-profit organisation, based in India, that undertakes interdisciplinary research on internet and digital technologies from policy and academic perspectives. Areas of focus include access to knowledge, intellectual property rights, openness (including open data, free and open-source software, open standards, open access, open educational resources, and open video), internet governance, telecommunication reform, digital privacy, and cybersecurity. Research at CIS seeks to understand the reconfiguration of social processes and structures through the internet and digital media technologies.

Australia-India Cyber and Critical Tech Partnership

This publication is the result of a collaboration between ASPI and CIS and was made possible with a grant under the Australia–India Cyber and Critical Technology Partnership from the Australian Department of Foreign Affairs and Trade (DFAT). ASPI and CIS would like to thank DFAT, Australia's Ambassador for Cyber and Critical Technology and the Australian High Commission in Delhi for their ongoing support.

This publication is ASPI's work, it was researched and developed independently and underwent ASPI's internal and external peer review processes. It does not necessarily reflect any policy positions of the Australian Government.

First published June 2024

ISSN 2209-9689 (online), ISSN 2209-9670 (print)

Published in Australia by the Australian Strategic Policy Institute

ASPI
Level 2
40 Macquarie Street
Barton ACT 2600
Australia

Tel Canberra + 61 2 6270 5100
Tel Washington DC +1 202 414 7353
Email enquiries@aspi.org.au
www.aspi.org.au
www.aspistrategist.org.au

Facebook.com/ASPI.org

@ASPI_org

Contents

Introduction

This techdiplomacy playbook offers an introduction to the processes of negotiation that underpin the development of technical standards for artificial intelligence (AI). In this report, we reflect on the role of technical standards, describe the current state of play in global AI governance and outline and explain *how* agreements on technical standards come into being.

Emerging, disruptive and critical technologies are increasingly taking centrestage in our lives. The future of work, the nature of our economy and geopolitical relations will be shaped by our ability to master technologies such as AI, quantum technologies, biotechnology and 6G. Critical technologies are now foundational to states' future economic and commercial prosperity, their political and diplomatic influence, their national security and ability to project future military power.

The transition of AI technologies from 'experimentation' to global use came to the fore in 2022 with the introduction of OpenAI's AI-powered language model, ChatGPT. ChatGPT's filtered but indiscriminate use of internet data[1] and widespread public take-up showed us a glimpse of how transformative AI technologies could be to future economic and business models, work and employment, and in meeting major societal challenges, from monitoring and predicting the effects of global warming to improving health care and access.[2]

But those same technologies are also seen to bring challenges and major potential risks if not managed and governed carefully and openly. Those risks range from violations of privacy and intellectual property rights to the amplification of embedded discrimination through to sophisticated manipulation of data and information.[3] At its most extreme, large-scale misuse or misgovernance of AI technologies could rock the foundations of societies, systems of government and international peace and stability.

Some are even concerned AI threatens our existence, as it's believed that some forms could surpass human intelligence.[4] That led leading scientists and experts to craft a warning, saying that 'mitigating the risk of extinction from AI should be a global priority alongside other societal-scale risks such as pandemics and nuclear war.'[5]

At the heart of how AI technologies are developed, deployed and used in a responsible manner sit a suite of technical standards: rules, guidelines and characteristics that ensure the safety, security and interoperability of a product.

Bridging the worlds of diplomacy and technology

As emerging, disruptive and critical technologies have become focal points of global competition, their management and governance have also turned into sites of contestation. In recent years, government leaders and international institutions such as the Organisation for Economic Co-operation and Development (OECD), the UN Educational, Scientific and Cultural Organisation (UNESCO), the UN General Assembly and the European Union (EU) as well as groups such as the G7, G20 and the Quad (Australia, India, Japan and the United States) have each prepared their interpretation of responsible AI.

In parallel, in the technical domain, companies and AI pioneers have introduced their own working principles, guidelines and standards that inform the work of product-development and sales teams.[6] While they experiment with the technology, introduce AI-powered applications to the market and engage in takeovers and mergers, the boundaries of current-day ethics, rules and standards are being tested and questioned.

The two worlds—of diplomacy and technology—come together (techdiplomacy) when negotiating updated and new technical standards. It's in the arena of technical standards-setting where governments, regulators, industry representatives and researchers hash out the details of what responsible use, deployment and governance of AI should mean, how it should be implemented and how it should be monitored and verified.

Effective negotiations require that participants have an understanding of the topic at hand, of the stakeholders and parties to the conversation, their constituencies, priorities and interests as well as the processes of 'getting to an agreement'.[7] They also require governments to ascertain whether their countries need to be part of that conversation, and in what way or form.

Given the high impact of AI on our societies and the crucial foundation role of technical standards, we believe that exchanges, more dialogue and greater collaboration between policymakers, technologists and civil society on technical standards for AI has never been more important.

This playbook helps key stakeholders step through the different aspects of negotiating technical standards for AI and should serve as an encouragement to get involved.

The playbook contains six chapters:

- Chapter 1 (pages 7–10) explains the essential role played by technical standards.
- Chapters 2 and 3 (pages 11–27) outline the emerging AI global governance framework, various instruments of governance (including, for example, regulatory legislation and technical standards) and the role of standards-development organisations.
- Chapter 4 (pages 28–35) offers a deep dive into key roles, leadership, governance and decision-making steps for current standards initiatives on AI. It presents graphical data on leadership and participation, by country.
- Chapter 5 (pages 36–43) examines the landscape of Indo-Pacific diplomacy in AI governance and looks at strategic policy settings for key Indo-Pacific nations and regional organisations.
- Chapter 6 (pages 44–46) outlines eight recommendations and steps to help inform and build an Indo-Pacific agenda for AI techdiplomacy.

Why this playbook? And why AI technical standards?

The idea of a techdiplomacy playbook emerged during 2021, when the Australian Government launched its International Cyber and Critical Technology Engagement Strategy and articulated ambitions 'to increase efforts to shape global standards' and 'to engage with international partners and recognised standards development organisations'.[8]

Identifying a policy ambition is one thing; doing something to effectively fill that gap takes planning, coordination and resourcing.

Early work undertaken by ASPI on this issue, and engagement with relevant stakeholders in and outside of government, led to discussions about whether policymakers and civil-society representatives understood the sometimes opaque and complicated world of technical standards and standards-making well enough to engage with standards bodies effectively.

At the same time, Australia and India intensified their discussions on cyber and critical technologies standards through the Quad,[9] with a view to supporting technology maturity across the Indo-Pacific.

With those developments in mind, ASPI and CIS joined forces and developed this playbook as an accessible introduction to the complicated world of AI technical standards.[10] Over the course of 2022 and 2023, ASPI and CIS consulted a diverse range of stakeholders in India and Australia on AI regulation, including government agencies, experts from standards-developing organisations (SDOs) and national standards bodies, academics, industry representatives and civil-society groups. Our consultations explored AI standards-development processes and the main players—particularly the evolving role of governments in standards setting.

Our consultations made clear that, despite growing engagement with standards and standards bodies, policymakers and technologists have only a partial understanding of how those entities and processes function, particularly in the emerging sphere of AI standards. Confusion remains about how AI standards fit into the range of global regulatory rules and principles being established to govern or regulate AI technologies.

Our mission was to take these complex AI standards-setting processes and present them in a manner that's digestible and accessible. This playbook aims to bridge the divide between the world of diplomacy, negotiations and multilateral talks, and that of technologists, industry and standards bodies. It's also intended to support policymakers and technologists from emerging Indo-Pacific economies. It's essential that their interests and needs are as well represented in multilateral and multistakeholder governance arrangements as those of industrialised and technologically advanced nations.

Having read this playbook, you should be able to:

- *recognise* the opportunities and gaps in the current patchwork of government-led and industry-driven initiatives that make up the current global system of AI governance
- *understand* the foundational role of technical standards in establishing and implementing any form of governance, whether subnational, national, regional or global
- *understand* the roles and responsibilities of national, regional and global standards-setting bodies and the principles and processes that underpin internationally recognised technical standards for emerging technologies
- *determine* where and how governments are best placed to engage in international rules- and standards-making initiatives.

A glossary of terms is at the back of this report.

Chapter 1: The essential role of technical standards

Standards are really boring, but really, really important.

—Ian Levy, former Technical Director at the UK National Cyber Security Centre[11]

The technical rules, guidelines or characteristics that ensure the safety, security and interoperability of technologies are typically codified in the form of technical standards.[12]

Those documents are frequently described as 'technical' and 'apolitical'—a sentiment strongly represented among technologists and academia. However, it's important to remember that standards are constructed by people and therefore inevitably reflect the beliefs and values of the people, organisations, countries and cultures debating and negotiating their final form.

Equally, standards are influenced by the current state of technology and the contemporary architecture of global governance.[13] AI governance is a live issue. As the EU's AI Act (2024) comes into force, the US President's executive order on 'Safe, secure and trustworthy AI' (2023) is implemented and China enforces its basic safety requirements (2024), the next phase of AI governance will increasingly focus on technical standards.[14]

That's the reason why diplomats, regulators, industry and civil society are currently so focused on 'getting the appropriate standards', 'getting those standards right' and 'setting them at the right bar'. Competing views and interests about what's appropriate and 'right' stem from:

- the competition between the US and China to maintain or acquire a technological edge in emerging technologies such as AI
- the intent of industry stakeholders to ensure that their practices or patented technologies become *the* standard
- the many other actors who want to protect their society, their markets, or both, on issues such as personal data and privacy, consumer rights and market competition.

Understanding the role of technical standards is fundamental to understanding an important instrument of governance for emerging technologies, particularly AI.

By the end of this chapter, you'll know more about:

- what technical standards are and what role they play in the AI global governance landscape
- what's driving the development of standards, and the main actors and institutions involved
- the different mandates, roles and responsibilities of SDOs.

What are technical standards?

A technical standard is defined as 'a document, established by a consensus of subject matter experts and approved by a recognised body that provides guidance on the design, use or performance of materials, products, processes, services, systems or persons'. [15]

In the context of AI global governance (and of technologies more broadly), there are three important elements to note:

- Standards are 'established by consensus', which means that a global multistakeholder community is largely in agreement with the proposed requirements and sees a need for that standard to exist—it fills a gap in 'the market'.

- Standards are developed by 'subject matter experts', which implies that ultimate decisions on requirements aren't driven by political and policy considerations but by technical soundness.
- Standards are 'approved by a recognised body', which suggests that there are institutionalised processes for the design, approval, maintenance and publication of standards.

That's what ideal standards and standards-development processes look like. It's been shaped by decades-long practices of standardisation in the US and European economies.[16]

Drivers of standards

Historically, the development of standards has relied on industry groups in Western liberal market economies—such as the Institute of Electrical and Electronics Engineers (IEEE), the World Wide Web Consortium and the European Committee for Electrotechnical Standardization (CENELEC)—to take the initiative, while governments respect the autonomous character of the standards-development process. They don't direct the outcome or own the process. That's different for many emerging economies, in particular those that only recently liberalised their markets, such as China, Indonesia and Brazil. There, the standards-making process has involved government bodies setting mandatory compliance standards for industry. Therefore, today, the drivers of standards involve a diverse and hybrid mix of entities that could be private, commercial, non-profit or public-sector groups, statutory agencies or membership-based organisations.

Types of technical standards

Technical standards come in a variety of forms, which can be classified according to their incentive structure, the 'object' of standardisation and their general availability:[17]

- *Network standards* are standards designed to enable coordination between parties to enable interoperability. Examples include standards for 5G, Wi-Fi or the Internet Protocol (IP).[18] There's little need for regulatory interventions to enforce compliance, since parties are self-incentivised to comply. If not, they'll place themselves 'outside of the market'.
- *Enforced standards*, on the other hand, require some form of external pressure to be developed and subsequent enforcement to ensure that they're followed.[19] Examples include standards for product safety and security that are mandated by national or subnational governments, either through regulation or as preconditions for government procurement, such as seatbelts in cars or workplace health and safety.
- *Product standards* relate to the specific requirements that a product must meet for things such as its functionality, safety and labelling (such as ingredients, care instructions or health warnings).
- *Process standards* outline requirements related to the process of production, testing and management of a product or service.[20] An example is the ISO 27001 standard for cybersecurity, which outlines the risk-management processes that organisations must follow.

These technical standards represent a good cross-section of the technical standards in actual use. Most of them are *open standards*: in principle, anyone can access, adopt and implement open standards, although sometimes for a fee or through licensing agreements. These are also the most foundational standards, based on which companies and developers can build their products and services. Most internet standards—such as HTTPS, DNSSEC and TLS[21]—are open standards. Open standards are also the standards that governments can include in regulations without breaching their commitments under (free) trade arrangements.[22]

On the opposite end of this spectrum we find *proprietary standards.* These standards are undisclosed, owned by single companies and often considered to be trade secrets. Microsoft's operating system,[23] Google's search algorithm[24] and Huawei's 5G patents[25] are examples of proprietary standards: clients use them openly, but don't have access to investigate or validate them. Given the market size of those companies and their products, and/or their inclusion in export promotion schemes, such business-owned proprietary standards frequently emerge as *de facto standards*, ahead of regulation.

Incentives for standards development

De jure and *de facto* technical standards are often considered to be *the* standards because they've been taken up by the market. That's another feature of technical standards: their use is in principle voluntary and non-binding and predominantly driven by a commercial demand unless included in legislation.[26]

Obviously, technical standards don't appear organically or in isolation. They're the result of a long negotiation process, which can often be —in Ian Levy's words— 'really boring'. In this section, we outline some of the main drivers of technical standards development. This is important because it reflects industries', governments' and other stakeholders' core interests, and why they're willing to invest their costly time and resources.

Commercial interests

Companies are primarily driven to develop international standards because they enable market access, provide a platform for innovation and can help reduce the costs of manufacturing. Companies that operate globally across national boundaries, such as tech companies, save significant time, expense and effort if their products and services are designed to a single universal standard, rather than needing to comply with multiple jurisdiction-specific and diverging standards. There's also a commercial benefit if companies can ensure that their own standards emerge as the universal norm or promote their proprietary assets as the essential underpinnings of an international technical standard. In such a scenario, a company can make a return on its initial investment in R&D from royalties and licence fees. These are known as *standard essential patents* (SEPs).[27]

Promoting their patented technologies as part of a technical standard allows patent-holding organisations to monetise their intellectual property.[28] In the area of ICT and emerging technologies, standards compliance will almost certainly require using a SEP: around 55% of ICT standards are patented technology.[29] While SDOs require SEP holders to commit to granting licences on fair, reasonable and non-discriminatory terms,[30] the interpretation of those terms is broad and contextual, and compliance has proven difficult to enforce.[31] At the country level, an economy that's able to convert domestic industrial standards into international standards gains huge economic value.[32]

Incentives from the multilateral trading system

Another driver of international technical standards is the multilateral trading system of the World Trade Organization (WTO), which is based on non-discrimination, lowering trade barriers, fair competition and transparency. The WTO uses conformity with internationally agreed technical standards as a benchmark to assess whether governments are imposing potentially unnecessary and unjustified obstacles to trade.[33] Those stipulations cascade down to other trade agreements, such as the Comprehensive and Progressive Agreement for Trans-Pacific Partnership[34] and the Regional Comprehensive Economic Partnership.[35]

In 2000, the WTO's Technical Barriers to Trade Committee agreed to six principles that an international standard must fulfil to be accepted as a basis for justified technical regulations or conformity assessments:[36]

- *Transparency:* all interested parties must be able to access information on proposals for new standards.
- *Openness:* all WTO members must be able to participate in the standardisation effort.
- *Impartiality and consensus:* all relevant WTO members must be given meaningful opportunities to participate, and decision-making should be based on consensus.
- *Effectiveness and relevance:* standards need to be effective and relevant to meet regulatory or market requirements.
- *Coherence:* new standards shouldn't duplicate or overlap with existing other work.
- *Development dimension:* participation of developing countries in the standards-development process needs to be encouraged.

When there are issues or disagreements, they can be referred to the WTO's Technical Barriers to Trade Committee for review. For example, China referred the proposed EU AI Act to the WTO in 2022[37] on the basis that the Act would disadvantage Chinese AI technologies entering the European single market.

Interests related to public security and consumer safety

Public demands for safety and security have driven proposals for standards that ensure technologies are trusted—safe, reliable and secure—and verifiable. Governments and regulators are the main forces in developing such standards, stimulating compliance with standards through procurement requirements, certification schemes and auditing practices.

A good example is the development of the ISO 27000 series (2005), which now represents the global benchmark for cybersecurity.[38] The seeds of ISO 27000 were planted by the UK Department for Trade and Industry's Commercial Computer Security Centre, charged with creating evaluation criteria for IT security products and a code of good security practice for information security. The British standard, concluded in 1995, subsequently formed the basis for the ISO standards.[39]

For AI technologies, concerns over safety, security and resilience are only now starting to make their way into the public policy discourse. In the standards-setting community, consumer safety and public-security issues are currently addressed through work in the International Telecommunication Union (ITU) and the International Organization for Standardization (ISO) on AI applications in the health and automobile sectors[40] and more generally on data protection, personal data protection and privacy.

Maintaining the *status quo*

Standardisation is also used as a tactic to maintain a *status quo* and technological advantage. Once a standard is set, agreed, promulgated and adopted across jurisdictions, it's typically hard to undo or adapt, or to introduce competing standards. Agreed standards also create 'lock-in effects' and path dependencies for future products.[41] As such, they define the existing playing field for companies and innovators, whereas new standards would inevitably create new 'winners' and 'losers'.

For those reasons, many existing AI technology companies, individually and collectively, have been comfortable in calling on governments to establish 'AI-friendly' regulation now. In the main, governments have been willing to do so.[42] The Biden administration has mandated the National Institute of Standards and Technology (NIST) to act as a key initiator, convenor and coordinator for AI standardisation in the US,[43] while G7 leaders have begun the Hiroshima Process to show that 'democracies can act quickly to lead the way in responsible innovation and in the governance of emerging technologies'.[44]

Key takeaways

- Technical standards are foundational to effective governance, and that applies particularly to the governance of critical technologies such as AI.
- Standards development is a competitive space: there are commercial and national interests at stake, and those who can initiate and shape standards can achieve and maintain a technological, economic—and potentially strategic—edge over their competitors, whether other companies or other economies.
- Technical standards help to establish what's considered 'good', 'responsible' and 'appropriate' and the means to perform objective verification. As such, they inevitably also enshrine values and norms that have informed the technology up until that moment.
- It's important that governments monitor how AI standards are evolving, understand the implications, actively plan for and engage in standards negotiations where required and prepare themselves for the eventual adoption of those standards.

Chapter 2: The emerging competition over the global governance of AI

It is essential for democracies to work together … to develop technical and governance standards and norms consistent with our democratic values.

—Indian PM Narendra Modi at ASPI's Sydney Dialogue, 2021[45]

Technical standards are foundational to governance, but not the only means of governance. In this chapter, we look at the suite of governance instruments that governments have available, as well as the global context of AI governance.

At the moment, many governments are developing or rolling out national AI 'road maps' designed to reap the benefits of AI technologies and stimulate local industries, while simultaneously experimenting with regulatory frameworks designed to manage the safe integration of AI systems into their economies.

In the Indo-Pacific, for instance:

- India is drafting a Digital India Act that will include liability clauses for AI platforms that cause harm to people[46]
- Singapore has introduced Verify AI to develop testing tools for user organisations[47]
- Australia is considering 'targeted regulation' that would offer 'appropriate safeguards' to society[48]
- China has introduced a suite of regulations that involve mandatory registration of algorithms, security assessments and basic safety requirements[49]
- In the US, President Biden issued an executive order that requires companies developing large foundational AI models to perform safety tests and report the outcomes to government.[50]

National regulation and verification efforts need to be aligned with agreed international norms, standards and principles—and vice versa – to ensure the ongoing global interoperability of systems, products and services.

Alignment with international agreements also offers governments, regulators and industry predictability, safety and security. Those are fundamental anchors for governments, particularly for those that must navigate between competing technology powers, that have significant population numbers employed in 'jobs at risk', or that are poorly resourced to shape the direction of international diplomacy.

To start understanding current national, international, government-led and industry-driven governance initiatives, how they fit together and where technical standards feature, this chapter steps through:

- the characteristics of the current framework of global AI governance, including key stakeholders and initiatives
- the types of governance instruments being proposed—national and international
- some key strengths and gaps in the current global regime for AI governance.

Global governance of technologies

AI governance has become a hotly contested issue in the past few years: within and between states, within industry, and among technologists, lawyers and ethicists. Between 2018 and 2022, governments alone proposed some 10 different statements of principles, each of which attempts to set rules, norms or standards for 'responsible AI' (see page 17 for details):

- UNESCO
- the North Atlantic Treaty Organization (NATO)

- the European Union / European Commission
- the OECD / G20
- the Quad
- the US, China and other countries.

In July 2023, the UN Security Council held its first ever meeting on an emerging and disruptive technology. The 15 member states debated the impact of AI on international peace and security and stressed the need for dialogue and collaboration to address both risks and rewards.[51]

In March 2024, the UN General Assembly adopted a landmark resolution on AI. It encouraged governments and other stakeholders to develop measures for 'internationally interoperable identification, classification, evaluation, testing, prevention and mitigation of vulnerability and risks during the design and development and prior to the deployment of the use of AI systems'.[52]

Commonly expressed concerns focused on the possibility that intentional or inadvertent use of AI might cause harm to people and societies. AI systems are suspected of being:

- based on opaque and unaccountable algorithmic functions and trained on unrepresentative datasets, thereby producing results with entrenched and amplified bias towards or against certain groups in society[53]
- used in conjunction with weapon systems, which might allow for the use of lethal autonomous weapons without human control[54]
- used as a tool to conduct information warfare, disrupting the social fabric that holds societies and/or democratic systems of governance together[55]
- able to disrupt large swathes of the global workforce by replacing humans in performing routine, but also creative and intellectual, tasks in the knowledge economy.[56]

While government and industry leaders now share common ground in addressing global concerns about the misuse of AI, no single treaty, convention or declaration to govern AI is in sight. It's even debatable whether that would be desirable. Instead, it's more likely that an agreed and accepted set of principles and standards will emerge—among a large group of governments and non-government organisations—that will offer developers, commercial entities and governments certainty and predictability, while also offering a framework for accountability.[57]

Governance instruments for technologies

Nonetheless, states have a variety of mechanisms available to them. They include the following six governance instruments:

1. international rules and norms
2. principles and ethical guidelines
3. strategies, policies and road maps
4. legislation
5. use-cases and good practice
6. technical standards.

The nature, purpose and limitations of each of those instruments are outlined below.

1. International rules and norms

Examples	Actors	Mode of influence	Level of influence
Political declarations UN documents or proceedings	Governments	Setting international benchmarks	Global

Within the framework of international law, international rules and norms are expressions of shared expectations between states. They're articulated through political statements or intergovernmental consensus texts that articulate what states and other entities should and shouldn't do—but they aren't legally binding and can't be enforced. Nonetheless, they have discursive influence and can shape international agendas.

The recent UN Security Council meeting on AI is an example of norm-setting: it invited and encouraged governments to formulate their views on the applicability of existing international law and international humanitarian law to disruptive technologies, thereby drawing initial 'lines in the sand'.[58]

International rules and norms serve to prevent distrust between states about the potential misuse of technologies for political–military or economic purposes.

International rules and norms can also fill a (temporary) vacuum in domestic lawmaking; for example, when domestic regulatory frameworks and use-cases haven't been established or when the application of international law hasn't yet been clearly defined. There's growing acceptance that governments will seek to use agreed rules and norms to hold multinational technology companies to account and vice versa.[59]

Intergovernmental bodies—such as the European Commission (2018), UNESCO (2021), NATO (2021) and the Quad (2022)—have made extensive use of political declarations and consensus statements to express their views on rules and norms in relation to AI (see Figure 1 on page 17). In most cases, those international commitments preceded national action plans or road maps for AI governance.

Known limitations of norms are their voluntary and non-binding nature, the absence of enforcement mechanisms and generally abstract levels of agreement, which allow for ambiguous and subjective interpretation.

2. Principles and ethical guidelines

Examples	Actors	Mode of influence	Level of influence
Statements of intent	Governments Industry	Laying groundwork for institutional frameworks	Global or sectoral

Principles and ethical guidelines rely on stakeholders (governments, industry, or both) regulating themselves based on self-defined and non-binding statements of intent. They can include self-imposed means of compliance reporting. This type of governance can be effective in situations in which there's a need or desire to demonstrate responsibility without full transparency or in which third-party verification is infeasible in practice. Most multinational technology companies, including Microsoft,[60] Google[61] and IBM,[62] have introduced ethical AI principles.[63]

Using principles and guidelines can be an effective approach to governing AI technologies because:

- self-regulation offers flexibility to move along with changes in technology and societal demands
- governments don't have a monopoly on systems operating from within their borders and are unable to prevent AI systems using their citizens' data (or prevent their residents using AI systems)
- public authorities don't have the means to inspect or audit actual AI systems.[64]

In July 2023, US President Biden re-emphasised the US Government's reliance on industry self-regulation. Seven leading US-based AI companies (Amazon, Anthropic, Google, Inflection, Meta, Microsoft and OpenAI) agreed to his call to commit to voluntary safeguards and agreed principles of trust, safety and security.[65] In practice, self-regulation can fall short of

expectations, or fail to protect vulnerable groups, when commercial interests are prioritised.[66] Industry stakeholders have also been accused of promoting self-regulation to prevent legislative action and reduce their public accountability.[67]

A subsequent executive order by President Biden in October 2023 recognised that shortcoming and introduced a suite of new safety and security standards insofar as the President can unilaterally impose them. One example is a new requirement, under the existing Defence Procurement Act, for companies to disclose the results of security stress tests of their AI systems.[68]

3. Strategies, policies and road maps

Examples	Actors	Mode of influence	Level of influence
National documents	Governments Industry	Setting national political direction	National

Strategies, policies and road maps are national-level documents that set out a time-bound mission and vision. Governments, industry sectors and companies adopt strategies and road maps to articulate their principles, objectives, priorities, concerns, opportunities, resources and so on.

Developing a strategy or policy obliges governments to come up with a shared perspective, overcoming siloed approaches and bureaucratic inertia, and generates a discussion among key stakeholders, such as industry, civil society and academia. For instance, a national cybersecurity strategy is seen as a demonstration of maturity.[69]

However, strategy and policy documents tend to be political and time-bound and connected to the specific administration, regime or leadership team launching them. In situations in which such strategies are unlikely to survive electoral or appointment cycles, other stakeholders are less inclined to follow. Many strategies and road maps in the technology domain also suffer from a limited understanding of the complexities of implementation and/or adequate financial and human resourcing to both implement and maintain them.

Chapter 5 of this playbook (page numbers 36-43) refers to several national strategies and policies for AI governance and technical standards.

4. Legislation

Examples	Actors	Mode of influence	Level of influence
Proposed legislation (Act / Bill / executive order)	Governments	Setting enforceable requirements	National

National or subnational legislation is one of governments' most powerful governance tools. It's a means to define specific norms or standards and ensure compliance with them, by means of civil or criminal punishment for violations. The EU's AI Act is the most advanced example of such regulatory intervention with presumed extraterritorial effects.[70] Few other governments have adopted AI legislation to date, although many governments in the Indo-Pacific prefer to regulate emerging security issues ('regulatory reflex').[71] For example, the Australian Government is considering mandatory guardrails for AI development and deployment in high-risk settings.[72]

The purpose of legislation and regulation is to provide clarity on what government, commercial entities or individuals should do or refrain from doing. The main point is that government can enforce laws and regulations through the judicial system.

However, legislative and regulatory action in the fast-moving technology sphere comes with specific challenges. Legislation takes time to negotiate and pass parliaments (years, rather than months); must be sufficiently well drafted to be both implementable and enforceable; and must take unknown future technological developments into account. Because AI technologies are increasingly ubiquitous, they can't always be regulated, or regulated equally.

If governments regulate AI technologies before sufficient use-cases have developed (*ex ante*), that may create an adverse effect: some risks might be overlooked, whereas others might be overstated. If governments wait too long and regulate after use-cases have been formed (*ex post*), that might be too late to prevent fundamental rights—such as privacy—from being infringed.

One school of thought argues that legislation and regulation stifle innovation. In practice, that isn't automatically the case but tends to depend on the market, the type of regulation and the type of innovation.[73] In some cases, regulation has encouraged innovation or provided enabling circumstances for innovation by providing investors with certainty, boosting consumer confidence, and steering investments to social-value R&D. Recent examples include regulations designed to meet green energy and net-zero ambitions and the forced unbundling of 'locked-in' hardware and software sales.[74]

5. Use-cases and good practices

Examples	Actors	Mode of influence	Level of influence
(Technical) reports Academic research	Government Industry Civil society—research community	Setting baselines before standardisation, and before rules and norms are fixed	Global or sectoral

Few of the governance instruments listed above could be developed without well-documented use-cases and good practice. Good policy is based on evidence- and data-driven research that diagnoses the core problem of an issue, and on designing and testing relevant, effective policy or regulatory interventions. In the pre-standardisation phase of a new technology, when the developers or owners of the technology still need to define standardisation requirements and build a community of support, most effort goes into documenting use-cases and good practices that will then form the basis for future rules, norms and standards.

Investing in use-cases and good practice aims to test the requirement for and effectiveness of standardisation or legislative and regulatory interventions. Documentation can look at the technology itself (for instance, safety prerequisites) or at the operating environment of the technology (for example, whether unfair competition or monopoly dynamics are operating in the market).

Singapore's Model AI framework is an example of a governance instrument based on good practices identified in other disciplines and foreign jurisdictions.[75] Based on internationally agreed principles laid out by the OECD, the IEEE, the US NIST and the EU, Singapore's Ministry of Communications and Information constructed a nationally specific framework accompanied by a software tool that allows companies to check themselves against objective, verifiable benchmarks.[76]

6. Technical standards

Examples	Actors	Mode of influence	Level of influence
ISO, IEEE, Internet Engineering Task Force (IETF) and national standards and other publications	Government Industry Civil society—research community	Standards for market entry and product conformity	Global or national

Technical standards offer governments, industry and civil society another option to govern emerging technologies. As outlined in Chapter 1, these standards address issues related to 'the technical core of AI'; they specify objective and verifiable product or process requirements with due deference to technical experts from industry and academia. Typically, they don't directly address political, social or ethical questions related to technologies.

Technical standards are developed at the national, regional and international levels. National or regional standards, such as those developed by the NIST or CENELEC in the US and EU, respectively, can be freely adopted by any other jurisdiction, thereby creating an extraterritorial effect.

As with some other governance instruments, technical standards tend to be used as a form of 'self-regulation', or co-regulation, since they rely on voluntary take-up. However, technical standards are also frequently embedded into regulations, international trade agreements and government procurement contracts.[77] Technical standards and the process of standardisation often emerge from the commercial (civilian) domain, although there's also a military component, such as NATO's standardisation work, including on a certification standard for responsible AI in the military domain.[78]

A complex regime of global governance is emerging

Over the past half-decade, the six types of governance instruments have been applied in different places—and semi-autonomously—by government and industry stakeholders.[79] They've often been applied in response to a certain incident or a major societal concern, or in response to market demands or concerns over maintaining or gaining a technological edge.

Although there's no consistent or predictable approach among governments or industries, it's useful to consider them all as part of one complex, overlapping, interactive and interdependent global regime of governance.

For instance, implementing legislation requires that technical standards have already been established, and legislative processes and subsequent decision-making are influenced by broader sets of agreed rules, norms and principles. Those rules, norms and principles are likewise dependent on consensus on the viability and soundness of the proposed safety, security and interoperability specifications. Those specifications are typically codified in technical standards.

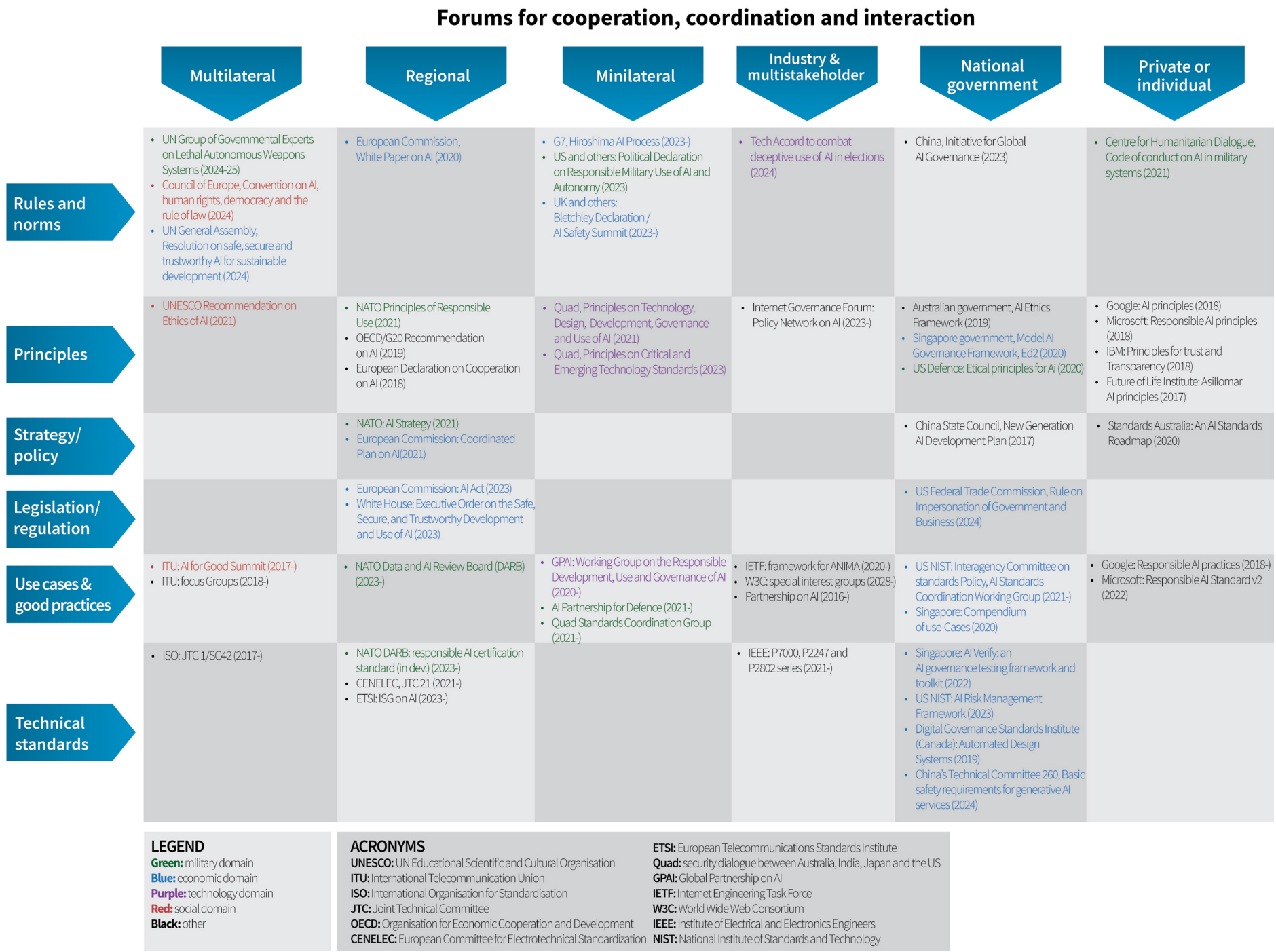
What does this regime look like?

Figure 1 maps:

- the different instruments of governance as articulated above
- the different groupings and forums wherein those instruments of AI governance have originated
- the primary domains of their application, such as economic, military, social or technical.

With that, we can observe the emergence of a complex regime of overlapping instruments of governance across a variety of domains (political, military, economic, social, technological) and driven by various state and non-state actor groupings (multilateral, minilateral, industry and individual).

Figure 1: The global governance of AI



The current state of global AI governance

It's evident that no common framework or dedicated platform for governments, industry and civil society currently exists to discuss the responsible development, deployment and use of AI. This isn't a unique situation, as the international community is grappling with this new and emerging phenomenon. Because of that, different bodies of varying composition are defining implications and requirements within their mandated areas of work. That creates this array of partially overlapping, mutually influencing but non-hierarchical initiatives (as illustrated in Figure 1).

Within this complex ecosystem, government and non-government stakeholders are compelled to address their interests either through a wide variety of existing forums or by establishing new initiatives—or sometimes both. This is a resource-intensive undertaking and tends to disadvantage newcomers to the space.

Some of the new(er) initiatives include the following:

- *The Global Partnership on AI* (GPAI), established in 2020 and currently chaired by India (2023-2024). The GPAI is a consortium of 29 member states that engages independent experts to undertake projects that would help members to better understand AI challenges and understand and shape AI opportunities.[80] During the first years of its existence, the group was hamstrung by competing views on its mission and purpose.[81] Recently, it's been repurposed to support the G7's *Hiroshima Process*, which is intended to develop 'guiding principles and an international code of conduct for organisations developing advanced AI systems'.[82]
- The joint Netherlands–Korea *Summit on Responsible AI in the Military Domain*. Following the inaugural conference in 2023, the organisers aim to establish a recurring summit that brings states together around a joint call to action (57 signatories) and supported through a Global Commission on AI.[83] In addition, the US presented its *Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy*, which 36 states subscribed to.
- The UN Secretary-General's 2023 *New Agenda for Peace*. The agenda makes recommendations on developing national responsible AI strategies; norms, rules and principles for military applications of AI; and a global framework for oversight mechanisms for the use of data-driven technology.[84] In parallel, the *UN Global Digital Compact* aims to build a framework to promote AI regulation based on accessibility, inclusion, responsibility, sustainable development and human-rights protection.[85] The UN Secretary-General also established an AI advisory body of individuals from industry, academia and government to build 'a global consensus' on the risks, opportunities and international governance of AI (see also chapter 4).[86]
- The UK-hosted *AI Safety Summit* in November 2023, which included announcements of AI safety institutes to be established in the UK and the US.[87] A follow-up summit took place in Seoul in May 2024 and it's presumed that this will become an annual event for like-minded partners to address 'frontier AI risks'.
- The Quad's 2021 *Principles on Technology Design, Development, Governance and Use* and 2023 *Principles on Critical and Emerging Technology Standards*. The governments of Australia, India, Japan and the US harmonise their approaches to technology and technical standards through the Standards Coordination Group, which is said to strategise the four governments' positions in standards-setting negotiations. Rather than being outward facing, the Quad arrangement is mainly effective in harmonising policy settings and approaches among the four members.[88]

The *EU's trajectory* is the clearest example of how one governance instrument can feed into another, ending up with a relatively comprehensive 'chain of technology governance'. It started with an articulation of principles (2018) and was followed by a White Paper (2020), an action plan (2021), a draft Act (2023) and a request of standardisation to CENELEC. The AI Act came into force in April 2024 with a two-year application period. (The next chapter looks at the role of standards-setting bodies such as CENELEC.)

Figure 1 also shows that efforts to date have concentrated on establishing international rules, norms and principles and on documenting use-cases and good practices. The centre of gravity for governance lies with regional organisations, minilateral groupings and national governments.

On the industry side, most established AI companies, such as OpenAI, Anthropic, Baidu and Tencent, have policies in place for usage, moderation and safety. Only a few, such as Microsoft and Google, have gone a step further. They've promoted their AI principles and accompanied them with the publication of responsible AI (technical) practices. Google was first to commence a process of annual self-reporting on their AI principles in 2019; Microsoft followed in 2024.

Those are important contributions to the global ecosystem, since many of those companies hold significant market positions and tend to be strongly represented in national delegations of standards working groups.

Key takeaways

- A lot of complementary and competing initiatives are currently underway; each is an attempt to define rules, norms and standards.
- None of them is conclusive or global, and it's uncertain which higher level governance initiatives—existing or new—will emerge as the most impactful, leading and credible.
- Regardless, the success of each of them will depend on agreed technical standards. Yet, the role of technical standards, and how they're formed, are the least well understood of all governance instruments.
- Standards often function 'under the radar', and technical standards-negotiation processes can be inaccessible and exclusive.

Therefore, the next chapter sheds some light on standards-negotiations processes and the main entities and roles involved.

Chapter 3: The playbook for negotiating technical standards

> *So today I want to talk to you about how we avert war and maintain peace – and more than that, how we shape a region that reflects our national interests and our shared regional interests.*
>
> *Those interests lie in a region that operates by rules, standards and norms – where a larger country does not determine the fate of a smaller country; where each country can pursue its own aspirations, its own prosperity.*
>
> —Australia's Minister for Foreign Affairs, Senator Penny Wong, 2023[89]

Most standards don't appear automatically or organically; they require 'entrepreneurs' who see a need and subsequently initiate and drive the development of a standard. They then require the broader community to come on board—to participate, engage and eventually subscribe to the standard.

As standards are an important part of the complex regime of technology governance, it's important for policymakers and technologists to understand how this system and community work. The main arenas for proposing and lobbying for new standards, and for advocacy and debate, are the international standards-development organisations.

SDOs operate as international organisations: they're headed by a secretary- or director-general acting under an assigned mandate with authority granted through participating members. They set meetings and venues and operate under charters and with codes of ethics and conduct.[90]

In this chapter, we describe the processes of negotiation on technical standards (with a focus on SDOs active in AI technologies), the main actors and the various roles in the standards-making negotiation process.

By the end of this chapter, you'll know more about:

- the main forums for standards development and their organising principles
- the main players and roles in a standards-development initiatives
- a breakdown of participants by organisation/country for the main AI standards bodies.

The main forums for standards development

There are hundreds of recognised SDOs, but for the purpose of this playbook we focus on four categories of SDOs, insofar as they have a role in the global governance of emerging, disruptive and critical technologies.

International standards bodies

International standards bodies (ISBs) are organisations active in developing global standards.[91] The most notable are the ISO, the International Electrotechnical Commission (IEC) and the ITU. The ISO and the IEC are independent, non-government and membership-based organisations. The ITU, on the other hand, is a treaty-based intergovernmental organisation with the status of specialised agency of the UN. Together, these three organisations form the World Standards Cooperation.

Except for the ISO/IEC Sub-committee 42 of Joint Technical Committee 1, which carries responsibility for up to 20 standards related to AI to date,[92] most bodies are still in a pre-standardisation phase for AI. At the ITU's 2022 plenipotentiary meeting, member states agreed on the need to work towards 'applying artificial intelligence (AI) technologies for good',[93] building on informal studies on the application of AI to health, autonomous networks, natural-disaster management and agriculture.

National standards bodies and national committees

National standards bodies (NSBs) and national committees (NCs) are national-level standardisation groups.[94] Their tasks are defined by each of their jurisdictions and may vary considerably: some are private, others are government; some have enforcement authority, whereas others are simply consultative.

NSBs/NCs serve two purposes: internal/domestic and external:

- Domestically, NSBs/NCs promote the adoption of international standards by domestic industry and/or develop nation-specific standards (Australian Standard – AS; Indian Standard – IS, Indonesian Standard - KBLI).
- Externally, NSBs/NCs represent their jurisdictions at the ISO, IEC and other international and regional SDOs.

Mirror committees

For AI technologies, many NSBs/NCs have set up 'mirror committees'—national versions of joint technical committees—and mobilise officials, industry representatives and academics. In some cases, NSBs/NCs have articulated national positions or road maps for AI standardisation, such as the National AI Standards Roadmap published by Standards Australia in March 2020.[95]

Great variety in NSBs

Domestic ecosystems for technical standards-setting vary greatly, as does the mandate for lead NSBs. In some jurisdictions, such as in the US, there's a widely distributed ecosystem with hundreds of entities at state and federal levels. In places such as India and China, there are single executive government agencies. In Australia and Europe, NSBs mostly involve membership-based bodies that operate under a government and social licence. The mandate of the NSBs and their resourcing ultimately determine how many seats they can acquire at the table, which leadership roles they can claim and for how long they can sustain that.

Regional standards bodies

Regional standards bodies (RSBs) play a similar role to the ISBs, but within the construct of a regional organisation. In Europe, where RSBs are most common due to the EU internal single market, there are CEN (the European Committee for Standardization; for all formal standards), CENELEC (for electrotechnical standards) and the European Telecommunications Standards Institute. In 2023, the European Commission instructed CENELEC to develop the EU AI Act's accompanying technical standards, ahead of the legislation's final phase.

No true RSBs exist in the Indo-Pacific, other than the consultation mechanisms of the ASEAN Consultative Committee for Standards and Quality and the recently established Quad Standards Coordination Group.

Independent SDOs

Independent SDOs are transboundary organisations that might not be formally authorised or endorsed by governments but effectively develop standards. The two most well known are the Institute for Electrical and Electronics Engineers Standards Association (IEEE SA) and the Internet Engineering Task Force (IETF).

The IEEE is an industry-driven membership association that develops industry-relevant standards for a range of industries, including AI, consumer electronics, robotics, power and many more, through a community-driven process.[96] The IETF is the premier SDO for standards related to the internet. Membership is voluntary: anyone can join the IETF's research and standardisation work (see case study on pages 25-26).[97]

The most active SDOs in AI standardisation

The most active bodies currently exploring standards for AI are the ISO, IEC, IEEE, ITU, IETF and CENELEC. Because so many of them are involved, an extensive web of arrangements exists that ensures coordination, deconfliction and the prevention of duplication. In principle, no new standards initiative should be accepted by any of the recognised SDOs if another is already ongoing or in existence.

Just as policymakers and technologists prepare for traditional forms of diplomatic outreach and international negotiations, it's important that they also understand how these standards organisations work, their mandates, their memberships and who fills key positions of leadership and influence.

Despite the great variety in SDOs and standards initiatives—public and private—they share common factors in the way they operate and gain credibility:

- They're all members- and participants-based: in principle, any stakeholder that has a vested interest can join, participate and contribute. Showing presence 'at the table' is an important way to contribute, as well as taking the initiative to lead and convene working groups, studies and other activities.
- Decision-making is consultative and typically based on consensus. While they follow an official process of initiation, drafting, consulting and finally decision-making, stakeholders that have core public or commercial interests at stake will be pressed to participate in the early stages of the process. As with all multistakeholder and multilateral negotiations, once a process is underway and has taken a certain direction, it's often difficult and costly to change course.
- In most cases, national standardisation bodies such as Standards Australia and the Bureau of Indian Standards (BIS) play a key enabling role. They mobilise, facilitate and coordinate multistakeholder communities of experts (government, industry, civil society and academia) in mirror committees. They also facilitate the formulation of national positions that feed into international standards bodies; they select representatives with a mandate 'to negotiate' and they feed international commitments back to domestic stakeholder groups.

In Table 1, we outline the leadership and governance details for each of the six bodies.

Private initiatives for standards

A final category to take into consideration is private initiatives. They're typically standards proposals initiated by individual companies or industry associations that don't find their way into any of the SDOs. They're common, but most fail to reach a critical mass of adoption or lack global impact. However, there are some exceptions.

Technology companies—those that are market leaders, that dominate in a certain technology area or are national flag carriers—can become *de facto* standards-setters. Examples include Microsoft's and Google's initiatives to introduce AI standards (see Figure 1 and case study below). Similarly, Huawei's technical standards for 5G technology were adopted across the global market, primarily because of Huawei's first-mover advantage.[98] As a most recent example, OpenAI—with the introduction of ChatGPT—can be expected to set the foundation for future technical standards for large language models.[99]

Table 1: The leadership and governance of standards-developing organisations in mid-2024

Name of SDO	International Organization for Standardization (ISO)	International Electrotechnical Commission (IEC)	Institute of Electrical and Electronics Engineers, Standards Association (IEEE-SA)	International Telecommunication Union (ITU)	Internet Engineering Task Force (IETF)	European Committee for Electrotechnical Standardization (CENELEC)
(Present) Leadership	Sergio Mujica (Chile)	Philippe Metzger (Switzerland)	Yu Yuan (China)	Doreen Bogdan-Martin (US)	Jay Daley (UK)	Elena Santiago Cid (Spain)
Membership	Open to a single national standard body per country. Third parties can participate through their NSBs. Currently 168 NSB members (participating and observing members)	Open to a single national committee (NC) per country Third stakeholders can participate through their NC	Open to individuals (who can't represent any entity or organisation) and corporates ('one company, one vote') Membership based on a range of corporate fees	Only open to member states. International and regional organisations, and industry can participate as sector member (for one sector) or associate member (for one project)	Open to all interested individuals No official recognition of representations of organisations, governments or industry	The national committees of the 27 EU member states, the UK, the Republic of North Macedonia, Serbia and Türkiye plus Iceland, Norway and Switzerland
Decision-making	One country – one vote 2/3 majority of all participatory (P) members + 75% of all members		75% of ballots returned & 75% 'yes' vote by eligible members	One country – one vote Consensus	Rough consensus	Consensus
Mandate	All industrial standards, including for technology	Standards for electrical and electronic technologies, such as fibre-optic cables	Standards for a wide range of industry applications, including electronics and telecommunications	Standards for various fields of telecommunications and ICTs, including smart cities	Standards for the internet	
Main operating bodies	Technical committees, subcommittees and corresponding working groups	Technical committees, technical subcommittees, and working groups	IEEE communities (technical and geographical) and societies (members-only) IEEE Standards Association working groups (open to anyone)	Working parties or study groups Once a submission is approved, it becomes a work item and has (an) editor(s) assigned	IETF working groups Internet Research Task Force (pre-standardisation work groups)	Technical committees and communities

Case study: Microsoft's Standard for Responsible AI

In early 2016, Microsoft's CEO, Satya Nadella, shared the company's first thinking about responsible AI.[100] In *Slate* magazine, he proposed six principles for the AI industry as well as some social principles that would support responsible AI technology:[101]

- AI must be designed to assist humanity.
- AI must be transparent.
- AI must maximise efficiency without destroying the dignity of people.
- AI must be designed for intelligent privacy.
- AI must have algorithmic accountability.
- AI must guard against bias.

He also posited that 'there are "musts" for humans, too.' Future generations will need empathy; education, knowledge and skills; creativity; and judgement and accountability. Microsoft established its internal AI, Ethics and Effects in Engineering and Research (Aether) Committee in 2017.

Developing an internal playbook

The Aether group refined Nadella's thoughts, which were adopted by the company in 2018. In practice, those principles didn't provide product groups and engineers with sufficient detail on how to apply and uphold them. In 2019, Microsoft established the Office of Responsible AI to ensure a comprehensive and coherent approach to responsible AI across the company.

In 2019, Microsoft concluded a first version of its Standard for Responsible AI. That internal playbook specified what Microsoft's AI principles meant in practice for its product teams. In 2022, Microsoft finalised an updated version 2 of the AI standard. This time, the document was made public and was accompanied by a toolkit that includes an AI impact assessment. Besides providing actionable guidance to product developers, Microsoft's standard also offers assurance to clients that the company is upholding its principles and filling a void in specific government policies, guidelines and regulations.[102]

The evolving landscape since 2016

Microsoft's AI principles have remained constant, even as AI technology has rapidly advanced and stakeholder expectations have increased. However, the governance, implementation and reporting mechanisms within the company have continued to evolve. The scale and scope of the Office of Responsible AI has increased to ensure compliance with internal policies, but also with ever-increasing requirements from government agencies, international standards bodies, regulators and think tanks. Also, a Responsible AI Strategy in Engineering (RAISE) group was established to assist engineering teams implementing commitments, principles and standards for responsible AI.

Examples

- *Commitment to NIST AI Risk Management Framework*. In January 2023, the US NIST published the AI Risk Management Framework,[103] which was mandated by Congress in 2020 under the National Artificial Intelligence Initiative Act. The AI Risk Management Framework came from a consensus-driven process involving government agencies, civil-society organisations and several technology companies, including Microsoft. Framework adoption is voluntary, but in May 2023 Microsoft committed to complying with the NIST's framework.
- *Support for developing regulation*. In 'Governing AI: a blueprint for the future' (2023), Microsoft made further proposals for an AI regulatory architecture, including the establishment of pre-deployment safety and security requirements and post-deployment monitoring and protection, as well as licensing for AI data centres for higher risk critical infrastructure systems.[104]

- *Transparency reports and certifications*. Good governance relies on regular, active reporting on progress against and compliance with referenced policies, agreements, regulations and expectations. Microsoft has indicated its willingness to comply with globally recognised AI certifications and reporting mechanisms as they're established and become available and appropriate, starting with transparency reporting on internal compliance in 2023.[105]
- *Global engagement.* In May 2024, Microsoft subscribed to the Seoul AI Business Pledge to draw of international best practices for safe, secure and trustworthy AI, including putting in place robust internal governance and risk management policies; and to a statement outlining eight commitments for 'frontier AI safety'.

Are current SDOs up to the task and demand?

SDOs are generally expected to be the main bodies for developing AI technical standards, but that isn't a given. Most of their current work on AI is still in the pre-standardisation phase. The speed at which AI technologies are developed and introduced into the market, and the 'general purpose' nature of AI technology, may prove too big a challenge for the current system of SDOs.

Standards-setting is characterised by extensive bureaucracy and procedural demands. The current SDO system might not prove agile and responsive enough to incentivise companies to push AI standards through standards bodies. Instead, the market may find that the technical standards for AI's constituent components, such as big data and data protection, risk management and cybersecurity, are sufficient.

Given the highly competitive commercial and geo-economic environment in which AI is currently developed and deployed, AI technology companies might also prefer to preserve their secret 'black box' proprietary AI standards, even if that leads to a splintering of the market. In such a scenario, global standardisation might jeopardise commercially sensitive information and a perceived edge in mastering the technology.

The lesson for policymakers is to make sure that they're across the ongoing work in existing SDOs and, where appropriate, direct new initiatives to the SDOs. However, they should also be mindful of the challenges that the system of SDOs faces and carefully monitor any new initiatives, including those outside of conventional bodies and groupings. The history of the formation of the IETF in the late 1980s offers a historical case in point. From a small group of technologists in 1986, it became *the* global standards-setting body for the internet.

Case study: The history of the Internet Engineering Task Force

This history of the IETF is an example of how a niche group of technical experts who invented the internet and were invested in ensuring its interoperability created an entity that would eventually become the SDO for internet standards.

The first IETF meeting started with 21 US-based technologists in 1986. Six years later, in 1992, the Internet Society was formed as a non-government entity to provide 'an institutional home for and financial support for the Internet Standards process'. The mission of the society is 'to promote the open development, evolution, and use of the Internet for the benefit of all people throughout the world'.[106]

Today, the IETF meets yearly in equal rotations between North America, Europe and Asia/Australia; around 2,500 people attend. It has established a structure that includes the Internet Engineering Steering Group, the Internet Architecture Board, the Internet Assigned Numbers Authority and the RFC (Request for Comment) Editor and Publication Centre. The RFCs are *the* internet standards and follow a consensus-based development process similar to those of the ISO, IEC and ITU.

The IETF is an example of how a newcomer group became a globally recognised standards body. It was an initiative by a small group of technical experts in a particular jurisdiction with deep knowledge of and expertise in a new form of technology. While very technical, the IETF is now also an example of a standardisation entity that *does* embody certain values and norms: those of the 'open internet'. That wasn't contentious in the 1980s and 1990s but has become more so in the 2020s, as more states pursue sovereignty and control over the internet.

Although it's less likely that this will happen again today (AI technology is already too well known and impactful, and the group of architects is so much bigger), it's still possible that an alternative or niche forum may emerge as *the* body for the technical standardisation of an emerging, disruptive and critical technology such as AI.

The European Commission's request that CEN and CENELEC (two of the regional SDOs) develop technical standards for the EU AI Act may be a first move in that direction and may set the norm for further standards-making. Similarly, the G7's Hiroshima Process may emerge as a nucleus for AI-related norms- and standards-setting.

What are the main roles in negotiating AI standards?

Any country that will be affected by AI technologies or is invested in leveraging it for economic and technological progress has a strategic interest in being part of the processes that make up the global framework of AI governance.

Nonetheless, most countries won't play a leading role in AI governance, because they don't have an indigenous AI technology industry, lack political or policy incentives, or allocate techdiplomacy efforts elsewhere. We've noted that setting standards is a process-intensive exercise. It takes time to canvas support for an initiative, to arrive at common terminology, to agree on technical requirements, and finally to generate global acceptance and take-up. There's a great deal of due process.

It will still be important for those countries to know the main players and influential roles in the standards-making process and the key decision moments. That enables them to monitor the various negotiation processes on AI standards and decide which individuals, roles or processes to engage for information or to shape outcomes. It also helps to identify key countries with which to partner and collaborate, and which to carefully monitor. Table 2 gives an overview of key roles in standards-making processes.[107]

Table 2 Key roles in standards-making processes

Role	Description	Example
Initiators	These are the individuals or organisations that identify a gap in the market and take the initiative to study the feasibility of a new or revised standard.	The authors or sponsors of a proposal, project or text. This can be an NSB or RSB, an individual company or an industry collective.
Influencers	These are the organisations—and their representatives—that are important or critical to 'get on board' to reach a critical mass of support, that can decisively shape the course of a development or negotiation process, and/or that can serve as conduits between groups with different positions.	In most cases, these will be NSBs, individual companies or industry associations with credibility and weight. Their weight can be the result of their market position (major tech companies), the market they represent (for instance, the EU internal market) and/or their thought leadership.
Decision-makers	These are the organisations—and their representatives—that ultimately vote and decide on starting a standards-making process, determining the maturity of new or revised standards, and approving new or revised standards.	In most cases, this will include the senior representatives of the NSBs as well as the senior management team of the relevant SDO.
Gatekeepers	These are the holders of roles that are essential to the management of the standards-making and negotiation processes. They determine the time and location of meetings, set the agenda, uphold procedures, and hold the pen for minutes and draft texts.	In most cases, these roles will be played by a member of the international secretariat, but it's not uncommon for an 'initiator' to be the penholder.
Users	These are the eventual users of the standards, who can be represented by the NSBs, industry or consumer associations, market regulators or other government bodies.	These are often the direct member organisations; that is, the NSBs and their respective members (individuals, individual companies and industry associations).

The responsibilities and opportunities that come with these roles explain why some governments are keen to fill certain positions with their own nationals, who are often individuals seconded from a government agency or NSB. Our descriptions also show that it's beneficial and instrumental for techdiplomats to establish constructive relationships and rapport with people in influencer, decision-maker and gatekeeper roles. The importance of those roles is illustrated by one of China's unsuccessful attempts to introduce a new standard for the IP. In the case study below, we highlight both the actors and their roles in standards-making processes.

Case study: How Huawei's proposal for a new IP standard failed to follow the process

In September 2019, the ITU's standardisation arm (ITU-T) received a proposal for studies into a new IP.[108] The proposal's *initiator* was Huawei Technologies, supported by Chinese state-owned telecommunications companies China Mobile and China Unicom, as well as China's Academy of Information and Communications Technology (a think tank within China's Ministry of Industry and Information Technology).[109] Huawei called the project 'New IP'.

The idea of New IP is to introduce a new top-down design of the internet that would account for multiple forms of identification (besides an IP address) and the routing of "many nets", with a particular focus on accommodating what China's describes as the 'industrial internet'.[110]

The idea received sharp criticism.[111] Many established stakeholders (*users*) dismissed New IP as an unprompted effort to overhaul the current internet architecture, which is based on a domain name system (address book) and the TCP/IP.[112] New IP would introduce 'a new system of trust and authentication' in which telecommunications operators would gain power to control data traffic flows.[113]

Huawei (the *initiator/influencer*) subsequently renamed its initiative 'Future Vertical Communication Networks' and sought to pitch its research proposals in other ITU study groups. Nonetheless, the study groups—made up of government representatives (*decision-makers*)—concluded that the proposal wouldn't be discussed further until March 2022, when the next four-year study term would start.

With insufficient support from the user community, Huawei's initiative failed to gain momentum. In fact, a consensus formed that the proposal didn't meet a market or technical demand (*users*)—the first criterion for starting a new standards initiative. Furthermore, the consultative mechanisms between SDOs through their liaisons (*gatekeepers*) also agreed that the IETF, rather than the ITU, was the appropriate platform for discussing internet standards—and the IETF wasn't convinced of the merits of the New IP proposition.

The Chinese companies are believed to have pursued this initiative through the ITU because they had the tacit support of the ITU's then Secretary General Houlin Zhao from China (*gatekeeper*) and because it fitted China's ambition (*influencer*) to expand the ITU's mandate from that of a telecommunications agency to a that of a 'technology agency'.[114]

Key takeaways

- Knowing which organisations and individuals are driving standards initiatives—and with what agenda, mandate and constituents—should be a minimum requirement for any responsible government.
- There is also ample opportunity for countries to be represented, albeit through an NSB, and gain a seat around the table and take up leadership roles. This can involve representatives from government (national or sub-national), industry, civil society and academia

Chapter 4: International leadership in AI standards-setting

If you're not at the table, you're probably on the menu.

—Unnamed diplomat in Brussels[115]

In Chapter 3, we described the important role of decision-makers, gatekeepers and influencers in international negotiations and in standards-making. We also noted that initiators have a 'first-mover advantage'.

This chapter outlines which countries are most proactive and take up positions of leadership and influence. The focus lies on current international AI standards initiatives or standards-like activities of the ISO, ITU, IEEE, GPAI and UN. We also touch on China's Global AI initiative.

This outline allows us to assess the degree of involvement of Indo-Pacific nations. That involvement can be seen as a proxy indicator of the countries that have the greatest interests, are willing to invest time and resources and exert the most influence. That influence can be used through the power to convene the groups (dates, times, locations) and by taking up agenda-shaping and penholder/editor roles.

By the end of this chapter, you will know more about:

- the representation of countries, organisations and stakeholder groups in the main AI standards bodies.

International Organization for Standardization / International Electrotechnical Commission

Sub-committee 42 of the Joint Technical Committee 1 (JTC1/SC42), created in 2017, is the group responsible for standardisation in the field of AI within the ISO and IEC (Table 3). As we've noted, participants in ISO/IEC groups operate under mandates from their NSBs. Since 2017, the work of the subcommittee has been coordinated and chaired by the American National Standards Institute (ANSI). In 2022 and 2023, JTC1/SC42 managed to develop and update some 20 AI-related standards.[116] In that respect, it's the most productive group of those listed here.[117]

Table 3: JTC1/SC42 participants, April 2024

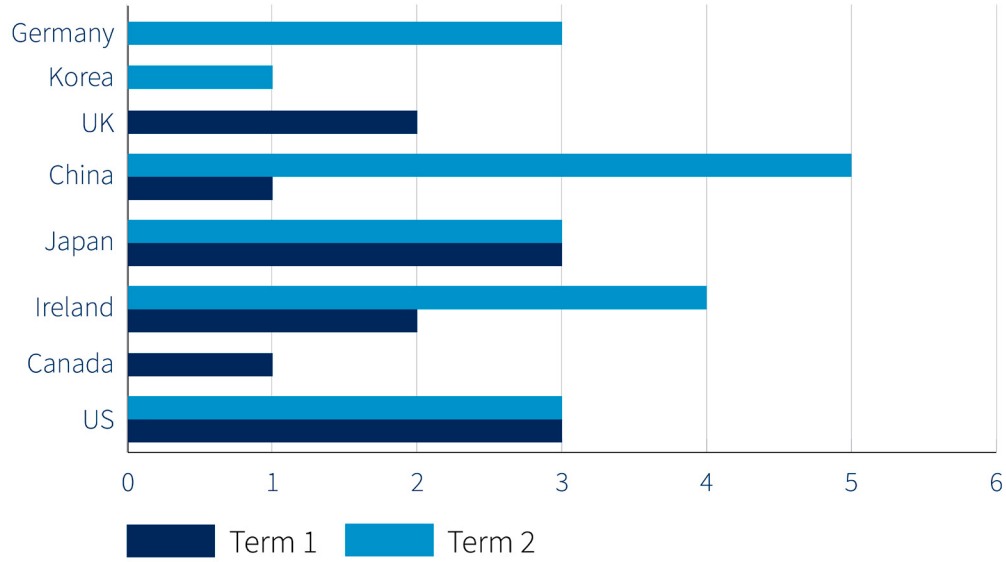
ISO/IEC JTC1/SC42	
Chair	American National Standards Institute (ANSI)—US
Committee manager	ANSI—US
Participants (name of NSB)	38 NSBs, including Australia (Standards Australia), China (SAC), India (BIS), Japan (JISC), Korea (KATS), the Philippines (BPS), Russia (GOST), Singapore (SSC) and US (ANSI)
Observers (name of NSB)	24 NSBs, including Indonesia (BSN), New Zealand (NZSO)
Conveners / secretariat (# of individuals; name of NSB)	Current term: Canada (1; SCC), Ireland (2; NSAI), Japan (2; JISC), China (1; SAC), UK (2; BSI), US (1; ANSI)
	Previous term: US (1; ANSI), Ireland (4; NSAI), Japan (2; JISC), China (5; SAC), Germany (3; BIN); Korea (1; KATS)

ISO proceedings involve a number of key roles: the chair of the subcommittee, who looks after the overall agenda, and convenors of working groups, who lead the work on specific studies or standards.[118] Typically, the initiator will take up the role of convenor and secretariat. Participating NSBs are required to 'play an active role', cast their vote on all official decisions, and 'base their positions on the consensus of national stakeholders', while observers only participate.[119] At the level of working groups, individuals technically function as independent experts.

The US has maintained leadership of JTC1/SC42 since the subcommittee's establishment. The US also chairs the parent Joint Technical Committee 1. Japan, too, has been consecutively involved in a convenor role. The terms of working groups typically last three years. Between the two terms, UK and Canadian experts initiated new working groups, while Chinese- and German-led initiatives came to an end.[120] Representation from the Indo-Pacific (excluding the US) has come from Australia, India, Korea, the Philippines and Singapore, all in a participatory role. Indonesia and New Zealand joined as observers.

This overview again shows that the Indo-Pacific region is a follower in the debate and that no Indo-Pacific standards bodies or experts are pushing any of their own initiatives or proposals (Figure 2). Even when indigenous AI capabilities in industry are well behind others, there's an opportunity for Indo-Pacific NSBs to incentivise greater academic participation, if only to monitor and inform.

Figure 2: Number of leadership roles in ISO/IEC JTC1/SC42, by nationality



Source: Data from 'ISO/IEC JTC1/SC 42: Artificial intelligence', ISO/IEC, May 2023, online.

International Telecommunication Union

The ITU's work on AI has been conducted in focus groups, which are *ad hoc* groups that respond to an acute perceived need but don't have a standardisation mandate from the member states. That means that their work isn't part of the official agenda and primarily involves 'pre-standardisation' activities: baseline research to assess the need, requirements and options for potential future standardisation.

The work of focus groups is self-organised and self-funded by the initiating member states, although they operate under the authority of a parent study group. Study groups are established by consensus by the World Telecommunication Standardisation Assembly, which is the governing body of member countries.

At the time of writing, the ITU (April 2024) runs three focus groups that deal with AI: AI for digital agriculture (from 2021), AI for national disaster management (from 2020) and AI for health (2018–2023, merged into the Global Initiative on AI in Health). Two completed AI-related focus groups dealt with the environmental efficiency of AI (2019–22) and AI for autonomous and assisted driving (2019–22).[121] In principle, focus groups shouldn't last for more than 12 months, unless their terms are extended.[122]

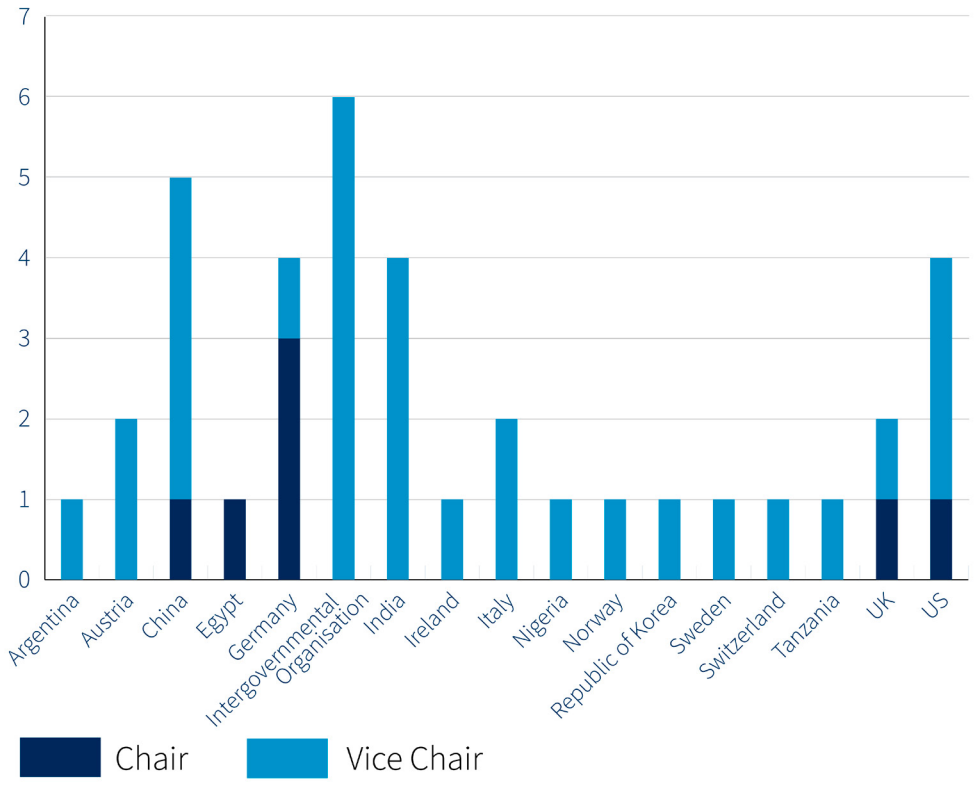
Table 4: The ITU's ongoing and completed focus groups on AI

ITU: Five focus groups on AI (ongoing and completed)	
Chairs	China, Germany, Egypt, the UK, the US
Vice-chairs	Argentina, Austria, China, Germany, Intergovernmental Organisations, India, Ireland, Nigeria, Norway, Republic of Korea, Sweden, Switzerland, Tanzania, the UK, the US
Process manager	ITU-T Bureau, Director Seizo Onoe (Japan)

Chairs and vice-chairs are appointed by the parent study group on the basis of 'demonstrated competence both in technical content of the parent group and in management skills'. The chair of the study group is also responsible for coordinating and deconflicting any work with other ITU-T initiatives. The role of chair is filled by member-state representatives and ITU sector members, while vice-chair roles can be taken up by ITU associates, academics and external experts.[123]

Our review of focus group publications shows that academia and civil-society organisations are the biggest contributors to the studies of the focus groups. At the same time, industry representatives hold the majority of chair and vice-chair roles. All focus-group participants operate with the consent of their member states (Figure 3).

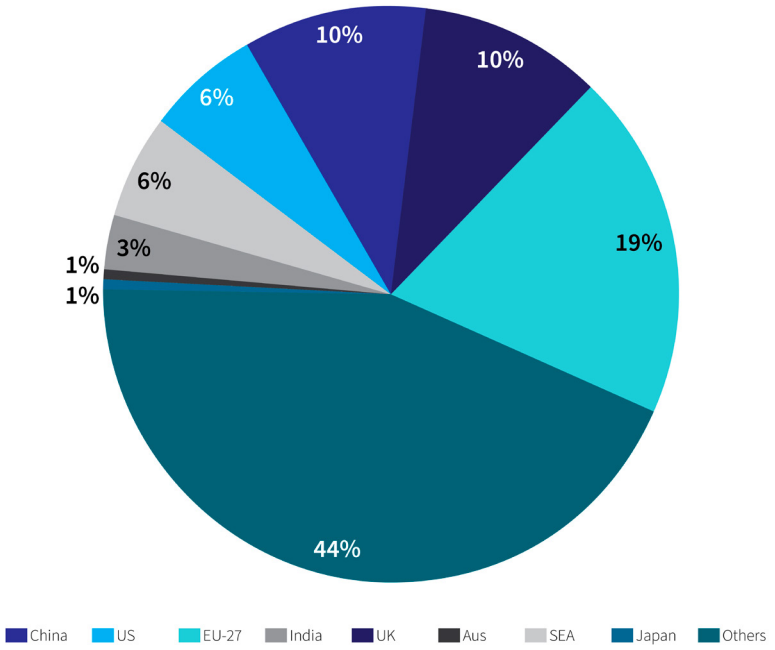
Figure 3: ITU focus groups on AI: leadership positions, by country



Source: Data from 'ITU-T focus groups', ITU, 2024, online.

Figure 4 indicates that the EU and the UK are the biggest single contributors to ITU-T studies, followed by China. Leadership roles (chairs and vice-chairs) of the five focus groups are held by China, Germany, Egypt, India, the UK and the US. For China, those individuals are employees of companies such as Huawei, the Telematics Industry Application Alliance, China's Academy of Information and Communications Technology and the China Telecommunication Corporation, and, for the US, by IBM, HP and John Deere. Germany's representatives are predominantly from the Fraunhofer Institute, which is Europe's largest non-commercial applied research organisation.

Figure 4: ITU focus groups on AI: contributors to studies, by country



Source: Data from 'ITU-T focus groups', ITU, 2024, online.

From the Indo-Pacific, besides the US, only India and Korea have held vice-chair roles. Of all studies produced for the AI focus groups between 2018 and 2023, contributions by Australian and Japanese authors each accounted for 0.6% of the total, India for 3.2% and Southeast Asia (that's Singapore) for 5.8%. Chinese authors have contributed 10% of the studies.

Member states are the main drivers of the work of the ITU. Indo-Pacific participation and leadership have been marginal, while Europe, China and US have led the debates. Given the multilateral nature of the ITU, there may be an opportunity for the Quad Standards Coordination Group to give greater voice to Indo-Pacific stakeholders in the ITU's pre-standardisation efforts.

IEEE Standards Association

The IEEE Standards Association is an industry-led group. Its committee on AI was established in February 2021 and looks at standards that 'enable the governance and practice of artificial intelligence related to computational approaches to machine learning, algorithms, and related data usage' (Table 5). In April 2024, it had 21 standards in draft and had completed three.[124]

Table 5: IEEE Standards Association Subcommittee on AI, to April 2024

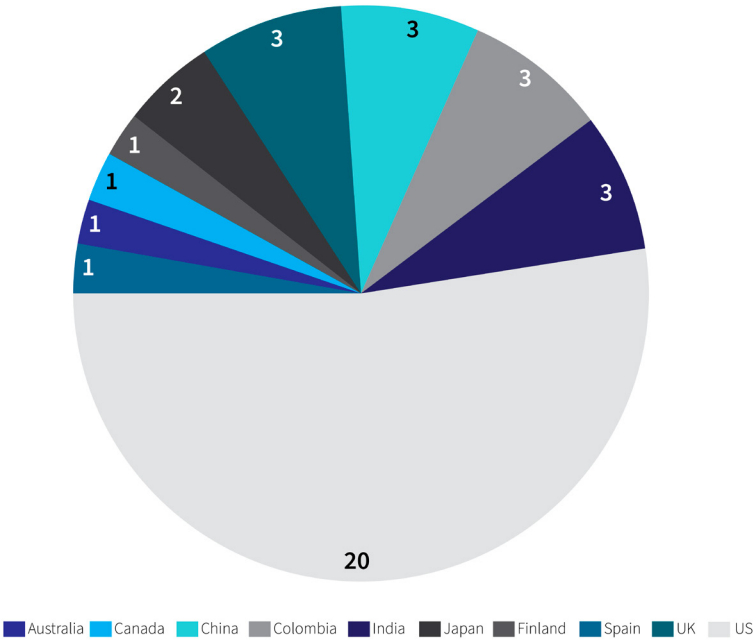
IEEE Standards Association Subcommittee on AI	
Leadership roles	Richard Tong (Chair; Chief Architect at Squirrel AI—China) Jeanine DeFalco (Vice-chair; US) Randy Soper (Secretary; US)
Initiators	19 project authorisation requests (PARs) are active at the moment, each led by a Chair.
Participants	31 participants acting in their own capacity on behalf of an organisation (company/university)

Source: 'Artificial Intelligence Standards Committee', IEEE Standards Association, April 2024, online.

Participants in the IEEE Standards Association are paying members and predominantly (96%) draw from industry and academia. While IEEE participants don't declare country affiliations, most of their institutional affiliations are with entities based in the US (37%) and China (18%) (Figure 5). Similarly, most initiators of IEEE standards initiatives are affiliated with organisations based in the US and China (Figure 6).

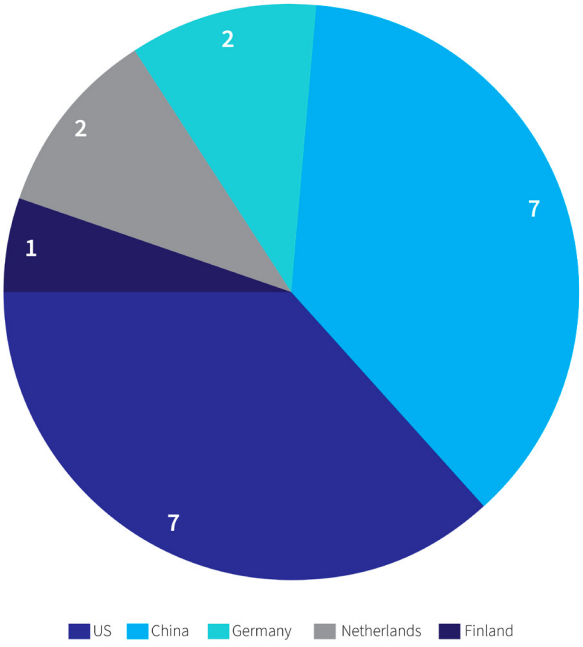
The IEEE's work on standards tends to focus more on compatibility and performance within specific sectors, whereas ISO and ITU work tends to focus on harmonisation among national standards-setters.[125] Therefore, the dominance of the US and China in IEEE AI-related work is a reflection of both countries' leading strength in indigenous AI capabilities (in research[126] and commercial applications).

Figure 5: Participants in IEEE AI standards initiatives



Sources: Data from 'Artificial Intelligence Standards Committee', IEEE Standards Association, April 2024, online; 'Active PARs', IEEE Standards Association, April 2024, online.

Figure 6: Leadership roles in IEEE AI standards initiatives, by jurisdiction



Sources: Data from 'Artificial Intelligence Standards Committee', IEEE Standards Association, April 2024, online; 'Active PARs', IEEE Standards Association, April 2024, online.

Other technical-expert-driven initiatives

While not intended to develop technical standards *per se*, the GPAI and the UN Advisory Body on AI are two experts-focused initiatives, outside of current conventional governance mechanisms, that may affect the future direction of AI governance and standards-setting for AI. Hence, it's worthwhile to assess those two efforts here too.

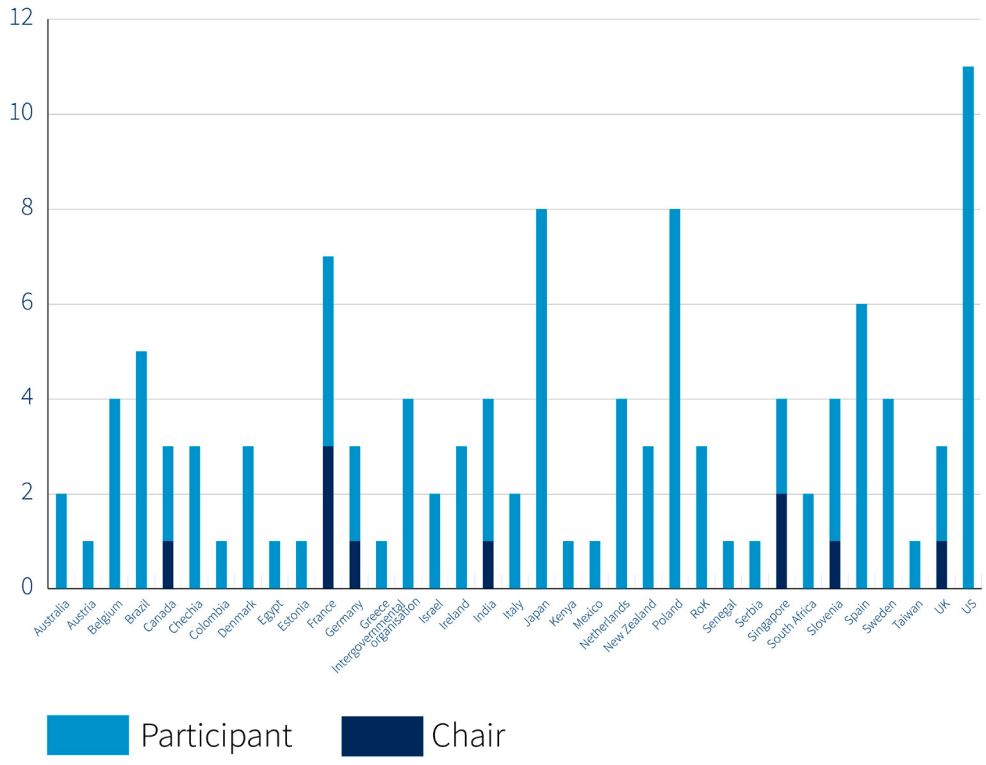
Global Partnership on AI

Formed out of a Canada–France joint initiative in 2018,[127] the GPAI was established in 2020 to 'bridge the gap between theory and practice on AI'. It's made up of member countries that bring together leading experts from industry, civil society, governments and academia. The GPAI is organised around the sharing of research and identification of key issues. Secretarial support is provided through the OECD, the International Centre of Expertise of Montreal for the Advancement of Artificial Intelligence and the Inria Paris Centre.

The chairmanship of the GPAI has been rotated annually, from Canada in 2020 to France (2021–2022), Japan (2022–2023), India (2023–2024) and Serbia (2024–2025). The GPAI was initially conceived as an AI version of the Intergovernmental Panel on Climate Change; that is, an entity that would provide scientific, technical and socio-economic evidence and analyses of impacts and future risks. Therefore, the group didn't intend to touch on AI governance or developing norms and rules.

By April 2024, 29 countries had signed up to the GPAI, and about 120 experts had joined by either nomination or invitation. An application to join is subject to endorsing the OECD Recommendation on AI (2019) or the GPAI terms of reference. The main work of the group is conducted by the participating experts, of whom ~21% represent Quad nations. From the Indo-Pacific, India and Singapore have taken up leadership roles in GPAI working groups (Figure 7).

Figure 7: GPAI chairs and participants, 2023, by country



Source: Data from 'What we do', Global Partnership on Artificial Intelligence, 2024, online.

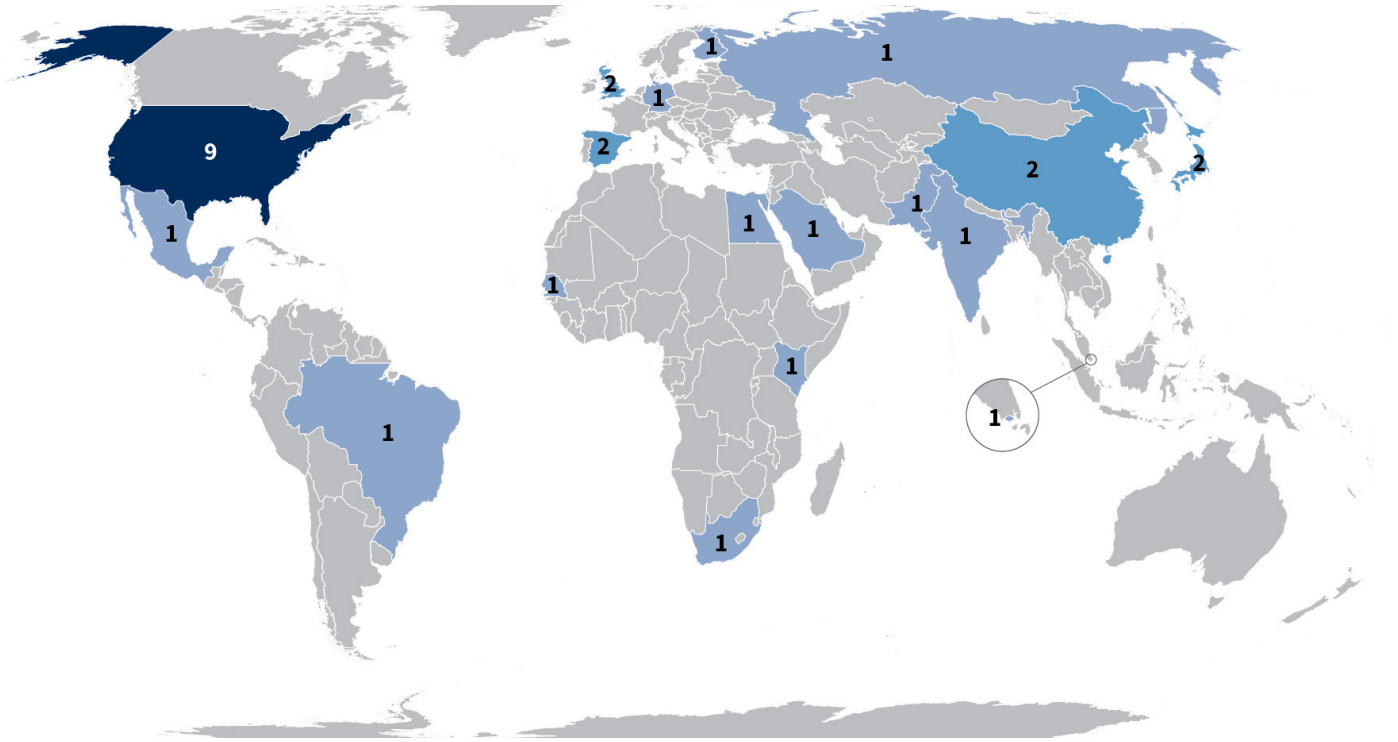
The GPAI is an example of a non-conventional initiative that may generate traction and gain credibility. In contrast to the previously discussed SDOs, there's a substantial level of representation from the Indo-Pacific, as experts from Australia, India, Singapore, Japan, South Korea and New Zealand participate. The G7's push for 'new AI guardrails', which is supposed to be channelled through the GPAI, may give this initiative a new impetus and opportunity for greater standards- and norms-setting impact.

UN Secretary-General's AI Advisory Body

In October 2023, UN Secretary-General Antonio Guterres established the AI Advisory Body of experts in the governance of AI or domains of AI application from government, industry, civil society and academia. In the months prior to the announcement, the UN had requested nominations from individuals as well as from member states' governments and reportedly received more than 2,000. Eventually, 39 individuals were selected from 25 different jurisdictions, including the Vatican.

Apart from Singapore, no experts from Southeast Asia or Oceania were selected (Figure 8). The US, as a jurisdiction, is the most strongly represented by people from six US-headquartered AI and tech companies, two academic institutions and a philanthropic organisation.

Figure 8: UN AI Advisory Body representation, by jurisdiction

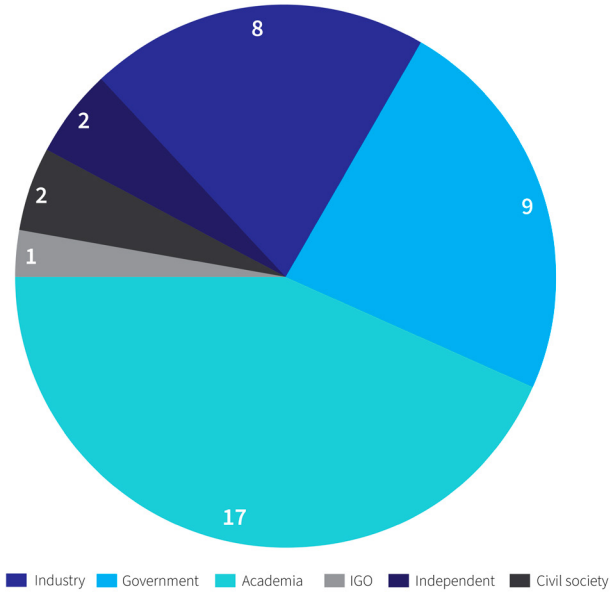


Source: Data from 'Members of the High-level Advisory Body on Artificial Intelligence', AI Advisory Body, UN, 2024, online.

The purpose of the body is to make preliminary recommendations on three areas: the international governance of AI; a shared understanding of risk and challenges; and key opportunities and enablers to leverage AI to accelerate the delivery of the UN Sustainable Development Goals. The recommendations will feed into the Global Digital Compact that the Secretary-General will present during the Summit of the Future in late 2024.[128] One goal of the GDC is to determine the role of the UN in the international governance of emerging technologies, including AI. A first interim report of the Advisory Body and a draft text of the GDC were circulated in April 2024.[129]

The body's composition is predominantly academic in nature (43%) (Figure 9). Governments and industry make up another 43%. The remaining minority (four experts) originate from civil society and include two unaffiliated independent experts.

Figure 9: UN AI Advisory Body representation, by stakeholder group



Source: Data from 'Members of the High-level Advisory Body on Artificial Intelligence', AI Advisory Body, UN, 2024, online.

China's Global AI Governance initiative

China's Global AI Governance initiative calls on 'all countries to enhance information exchange and technological cooperation … and develop AI governance frameworks, norms and standards based on broad consensus'.[130] Among other things, China believes that those elements should aim to:

- ensure social security and respect the rights and interests of humanity
- respect other countries' national sovereignty
- establish a testing and assessment system based on AI risk levels
- establish and improve relevant laws, regulations and rules, and ensure personal privacy and data security in the R&D and application of AI.

In contrast to the other initiatives listed here, Beijing's proposal didn't emerge from international consultations; nor was it intended as an initiative that others could feed into. It simply outlines China's viewpoints. The initiative does, however, signal China's strategic intent in regard to the global governance of AI and also offers context to China's 'on the ground' *de facto* standards-setting initiatives. Those include the network of 'smart cities' inside and outside of China enabled by China's tech giants' products[131], China's lead role in the export of facial-recognition technology, and activities such as the 'Luban workshops'—a global vocational training program that includes standards development.[132]

Key takeaways

- Many concurrent standards-related processes are currently underway. The bulk involve *preliminary* (pre-standardisation) work that focuses on establishing an evidence base of good practices. The *practical* development of actual international standards on AI still seems to be in a very early stage of progress and is concentrated in the ISO.
- Overall, the US and China seem to be leading the pack, followed by Europe. That's mostly due to the size, scope and resources of their national standardisation communities as well as their indigenous AI industrial bases.
- It's worth noting that the rest of the word, including the Indo-Pacific, is playing catch-up in most AI standards initiatives. GPAI is an exception: here experts from Australia, India, Japan and New Zealand have taken the opportunity to join in. It is concerning, however, that very few representatives from the Indo-Pacific – besides China and Japan -have been selected for the UN Advisory Body.
- Not being adequately represented is a strategic risk for countries in this region. After all, being part of the conversations and negotiations is everything, since 'if you're not at the table, you're at risk of being on the menu.'

Chapter 5: Indo-Pacific diplomacy in AI governance and standards

> *Tech diplomats are expected to be able … to interact with many different sectors, industries and innovation ecosystems, while seeking win–win cooperation with partners in frontier technologies to help promote economic and social development back home.*[133]
>
> —Eugenio Vargas Garcia, Deputy Consul-General and Tech Ambassador, Brazil

At the start of this playbook, we described how the world is currently laying the foundations of a global regime governing critical technologies such as AI, and how choices on standards will ultimately guide how AI is used and deployed internationally across jurisdictions.

Broad inclusion and representation are key to reaching consensus on international rules, norms and standards. At the same time, building global and multistakeholder agreement is a time-intensive and slow journey. As we explained in Chapter 1, to ensure that established standards are maintained, governments and industry will need to commit to them voluntarily and consistently. That will happen only when standards serve public and commercials interests alike, support economic growth and technological advances, and sufficiently reflect stakeholders' cultural, societal and organisational values and norms.

For those reasons, technical standards-making is a contested space. The standards-development bodies, where political values, institutional interests and technical specifications intersect, are critical sites for techdiplomacy. In Chapter 3, we saw that Europe, the US and China are currently leading the charge in establishing nationally, regionally and, at times, globally agreed standards for AI.

Jurisdictions in Oceania, South and Southeast Asia (and, to a lesser extent, Northeast Asia) are mostly 'price-takers'. They're on the receiving end of the outputs of international—or global—technology leaders' decisions on emerging technology rules, norms and standards. This isn't to suggest that those regions are oblivious to or uninterested in ensuring the responsible development and use of emerging technologies. Some countries have lacked political and/or bureaucratic leadership in this space; others have lacked the necessary human capital and resourcing needed to work in and influence it; some also lack sizeable indigenous technology industries that could provide expertise for a sustained period and would give them a seat at the table.

Overall, the capacity of Indo-Pacific stakeholders to engage in critical technology standards has historically been lower in comparison to other jurisdictions.[134] However, a price-taking posture for emerging and developing economies might no longer be desirable or defensible. For a region that's banking on the opportunities of a digital and technology-enabled economy and has large swathes of its population in at-risk jobs, it's a matter of national and economic security for Indo-Pacific stakeholders to have an adequate say in how AI technologies will operate and be used.

In this chapter, we first look at the positions that China, the EU and the US have taken on technology governance and the role of technical standards, followed by descriptions for Australia, India, Japan, Singapore and the Association of Southeast Asian Nations (ASEAN).

With that information, you should be able to:

- *identify* which governments hold convergent or divergent views on AI governance and standards
- *understand* how and why countries come to their positions and viewpoints.

Three global leaders in AI standardisation: China, the EU and the US

This section offers an overview of the most active governments' and regional organisations' interests and priorities in technologies; their positions on technology governance and standardisation for AI; and their preferred avenues for international engagement.

China

National interests and priorities	The 2017 AI Development Plan states China's ambition to become 'the world's primary AI innovation centre' by 2030, leading the world in foundational theoretical research, industry competitiveness, skills training and AI laws, regulations, policy and norms.[135] This aligns closely with the Made in China 2025 strategy, which aims to move China up the global value chain to become dominant in global high-tech manufacturing by 2025.[136] AI is recognised as one of seven frontier technologies in which China seeks to lead a breakthrough.[137]
Governance model for technology	China's model is described as 'government led; enterprise driven'. Its model for technology governance remains based on the centrality of the state, although industry's role has been elevated during the past decade: since 2014, industry bodies have been allowed to propose standards. At the same time, the Chinese Communist Party has asserted greater control over technology companies.[138] The relevant main entities are the Standardisation Administration of China, which leads on AI standards within the central government, supported by the National AI Standardisation General Group and the China Electronics Standardisation Institute. The Cyberspace Administration of China is an entity with a growing remit.
Objectives on technical standards	China's Standards 2035 Strategy (2018) emphasises the ambition to set global standards for emerging technologies. The accompanying 'National Standardisation Development Outline' argues for:[139] • greater engagement, including fulfilling duties in international standards-setting organisations and actively participating in international standardisation activities • stronger coordination between domestic and international standardisation. In February 2024, the Standardisation Administration of China released a standard on basic safety requirements for AI services.[140]
Objectives on (global) governance of AI	China is pursuing three distinct approaches to AI governance:[141] • algorithmic and information control, led by the Cyberspace Administration of China • testing and certification of trustworthy AI systems, led by the China Academy of Information and Communication Technology / Ministry of Industry and IT • establishing AI ethics principles and ethics review boards, led by the Ministry of Science and Technology. China's objectives rest on the idea of ensuring that international initiatives reflect domestic policy, regulation and standards.
Preferred forums for international engagement	Generally, China prefers to work through established UN and other multilateral organisations, such as the global SDOs. It also uses its arrangement with Brazil, Russia, India and South Africa (BRICS) and its Belt and Road Initiative to advance its positions and interests and introduce *de facto* standards. For instance, in October 2023, at the Belt and Road Forum for International Cooperation, President Xi Jinping introduced China's Global Initiative for AI Governance (see page xx).[142] Earlier, in 2022, China submitted a position paper on 'Strengthening ethical governance of AI' to the 2022 meeting of the UN Convention on Certain Conventional Weapons.[143] In February 2023, China endorsed a call to action for the responsible use of AI in the military domain.[144]

European Union

Interests and priorities	The EU's approach to AI governance aims to boost research and industrial capacity while ensuring AI safety and fundamental rights. Specifically, the EU aims to:[145] • 'provide enabling conditions for the development and uptake of human-centric, trustworthy, secure and sustainable AI technologies in the EU • make the EU a thriving place for AI research commercialisation • ensure that AI works for people and is a force for good, through talent and education programs, and a legislative proposal • build strategic leadership in high-impact sectors, including environment, health, robotics and transport.'
Governance model for technology	The EU's model is described as a 'rights-based approach' intended to protect citizens, in some cases against big-tech companies and states.[146] Therefore, its technology governance has focused on privacy and human rights, as well as unfair competition and antitrust actions.[147] As the EU's Executive Branch, the European Commission initiates AI governance initiatives with support from (among others) the High-Level Expert Group on AI, the Working Party on Telecommunications and Information Society, the Ad hoc Committee on AI and the European AI Alliance. CEN and CENELEC are the regional standardisation groups for the EU.
Objectives on technical standards	The EU's Global Strategy (2016) introduced the notion of 'strategic autonomy', which has since driven the EU's political, economic and military development.[148] It also informed the EU's Standardisation Strategy (2022), which lists five sets of actions:[149] • anticipate, prioritise and address standardisation needs, identified in the EU annual workplan and informed by a high-level forum • improve the integrity of European standardisation, which includes protection against undue influence of actors outside of the EU • enhance European leadership in global standards • introduce a 'standardisation booster' to EU-funded research and development • train the next generation of standardisation experts within academia. A Chief Standardisation Officer was appointed: Ms Maive Rute, the Deputy Director-General for Internal Market, Industry, Entrepreneurship and SMEs.[150]
Objectives on (global) governance of AI	The core component of the EU's governance of AI is the new AI Act. This legislation establishes obligations for providers and users depending on the level of risk that their AI application might pose. Risks are categorised as unacceptable, high and limited. Some applications may be banned from the EU, but others must undergo a conformity assessment and receive a Conformité Européenne (CE) marking before being placed on the market. Most AI applications are likely to be classified as 'limited risk'.[151] On the finalisation of the Act, the European Commission has tasked the regional standardisation organisation CENELEC to develop technical standards for this risk categorisation and subsequent conformity assessments. The EU's primary objective is the homogeneity and security of its internal market, but the AI Act is also likely to have a 'Brussels effect'.[152]
Preferred forums for international engagement	The EU supports multilateral forums but has recently opted to work through tailored structures such as its trade and technology councils with the US and India to advance the implementation and adoption of trustworthy AI. In 2023, the EU and the US agreed to jointly develop a voluntary AI Code of Conduct, which would include non-binding international standards on risk audits, transparency and other requirements for companies developing AI systems. Once finalised, it will be shared with G7 leaders as a joint transatlantic proposal, and companies will be encouraged to voluntarily sign up.[153] In addition, the EU has entered into 'digital partnerships' with Japan, Singapore and the Republic of Korea to foster cooperation in digital trade and to pursue alignment on the development and use of trustworthy and human-centric AI.[154]

United States

National interests and priorities	Executive orders on AI, issued under consecutive administrations by presidents Trump and Biden, aim to maintain and strengthen US leadership in frontier technology and state that the US 'must drive' technological breakthroughs in AI as well as in the development of appropriate technical standards.[155] The US has also introduced further steps that seek to revitalise 'domestic manufacturing, create good-paying American jobs, strengthen American supply chains, and accelerate the industries of the future'. AI is one of those industries and is boosted through instruments such as the CHIPS and Science Act (2022).[156]
Governance model for technology	In the US, industry, consortiums and other private-sector groups have historically driven technology governance. While support and assistance are provided through national standardisation bodies such as the NIST and ANSI, the model relies strongly on market incentives composed of self-regulation and voluntary principles. However, recent administrations have set policy directions that aim to coalesce American interests in a concerted manner, particularly on AI.[157] At the same time, individual states can also introduce legislation. By the end of 2023, 17 states had Bills detailing rules for the design, development and use of AI.[158]
Objectives on technical standards	The US Government National Standards Strategy for Critical and Emerging Technology (2023) stipulates that it's vital for the US that 'the "rules of the road" for critical and emerging technology standards embrace transparency, openness, impartiality and consensus, effectiveness and relevance, coherence, and broad participation'.[159] It lists the following priorities: • pre-standardisation research on innovation and cutting-edge science • standards development on topics of national security • lower barriers for participation in standards development for domestic stakeholders and from emerging economies • expanding presence in tech initiatives that touch on significant national interests and involve early-stage technology and related policy development. The US Government's Leadership in AI Plan (2019) suggests that the US will prioritise standards that are consensus-based; inclusive and accessible; nimble, multi-path and responsive to needs of developers and users; open and transparent; and result in globally relevant and non-discriminatory standards.[160] The plan deliberately avoids focusing on a single SDO since 'in fast-moving areas of technology such as AI, new standards initiatives are launched by existing—and new—organizations'.[161]
Objectives on (global) governance of AI	The US Government's objectives in governing AI are best articulated in the White House's 'Blueprint for an AI Bill of Rights' (2022), which aims to serve as a guide for 'a society that protects all people from these threats—and uses technologies in ways that reinforce our highest values':[162] • systems should undergo pre-deployment testing, risk identification and mitigation, and ongoing monitoring. • protect individuals and communities from algorithmic discrimination and ensure the use and design of systems in an equitable way. • stricter data practices compel AI technologies to seek permission before collecting, using, accessing, transferring and deleting personal data. • introduce documentation and explanation around when and how users interact with an automated system. • offer an opt-out and the option of a human alternative. On top of those measures, the US Government is invested in maintaining and protecting its edge in frontier-technology AI systems[163] (those technologies that can perform in a way that matches or exceeds capabilities present in today's most advanced models). Many of those objectives were subsequently reinforced through Executive Order 14110.
Preferred forums for international engagement	The US is an active and present participant in most multilateral forums, but it's most actively pursuing new initiatives in smaller bilateral and minilateral settings with allies and like-minded partners such as the EU, the Quad, ASEAN and the Asia–Pacific Economic Cooperation forum. As a member of the Quad, the US has subscribed to a common set of 'Principles on Critical and Emerging Technology Standards'.[164] The US also joined the UK in the Bletchley Park effort as they co-announced the creation of an AI Safety Institute.[165] The US takes unilateral actions at times, such as its issuing of the 'Political Declaration on Responsible Military Use of AI and Autonomy'.[166] For the US, the NIST is an important and influential entity. While focused on coordinating domestic standardisation, its products and standards have been taken up by foreign jurisdictions, including the AI Risk Management Framework that NIST produced in early 2023.[167]

Influencers from the Indo-Pacific: Australia, India, Japan, Singapore and ASEAN

Australia

National interests and priorities	For Australia, critical and emerging technologies are fundamental to its national interests. It considers some clusters of critical technologies (for example, in AI and sensing) to be driving broader data and digital transformation across the economy and society and breaking down traditional distinctions in the industrial-sector-based economy.[168] The Australian Government's 2023 'Critical Technologies Statement' aims to promote and protect technologies in order to:[169] • give Australians access to cost-effective, safe, secure and inclusive technologies • promote Australia as a trusted partner for investment, research and innovation • support regional resilience and competitive, trusted and diverse technology innovation • enable Australian industries to thrive and maximise their intellectual property. Australia is also concerned about these technologies because they form the centrepiece of competition between the US and China.[170]
Governance model for technology	Australia's governance model is based on principles and policy guidelines in which the federal government plays an enabling and facilitative role for industry, academia and civil society, in part through Standards Australia and other private associations. There's also an autonomous role for state and territory governments, which can drive their own governance arrangements. For instance, the New South Wales Government introduced the AI Ethics Principles and an AI Assurance Framework in 2022.[171]
Objectives on technical standards	In the 2023 Australian Cybersecurity Strategy, the government committed to 'work with industry to encourage the adoption of international standards' and take interim options to 'co-design options to legislate' mandatory standards.[172] Internationally, the government wants 'international standards for critical technologies [that] will reflect Australia's interests and expertise'. Furthermore, it says that 'Australia must do more with international partners to defend and strengthen the international standardisation system, advocating for our shared interests and amplifying regional voices.'[173] The 'Critical Technologies Statement' notes the need to 'proactively shape the design, development and use of critical technologies and their standards' as a key means to manage the risk of critical technologies, and ensure secure, resilience and transparent supply chains for critical technologies.[174]
Objectives on (global) governance of AI	The federal government wants to create 'a regulatory environment that builds community trust and promotes innovation and adoption while balancing critical social and economic policy goals'. It also seeks to ensure that 'the development and deployment of AI systems in high-risk settings is safe and reliable'. In formulating new regulative initiatives, it will 'leverage [Australia's] strong foundation and domestic capabilities to support global action to address AI risks'. In doing so, it will place 'people and communities at the centre when developing and implementing its regulatory approaches'. The National AI Centre will work with industry to draw up a single risk-based AI safety framework for the responsible adoption of AI for Australian businesses at home.[175]
Preferred forums for international engagement	Australia—through Standards Australia and the government's ITU representative—has traditionally been represented at the SDOs. It has also taken an open and active stance towards new minilateral initiatives that involve US and key Indo-Pacific partners, such as AUKUS, the Quad and various bilateral initiatives. • Examples include Australia's: • support for the UK-hosted Bletchley Park declaration[176] • lead on the Quad Principles on Technical Standards for Technology[177] • collaboration with Singapore to test both countries' AI ethics principles.[178]

India

National interests and priorities	For India, its achievements in science and technology are the subject of national pride. New, emerging and strategic technologies are means to support India's economic growth and indigenous innovation, expand market opportunities and solidify relations with the global South. This is bolstered by its membership of the G20, the Quad and the G7. India also sees standards, and compliance with standards, as a factor in achieving the status of a developed country.
Governance model for technology	The Indian Government primarily drives technology governance in India, in collaboration with various sectoral regulators. The Bureau of Indian Standards (BIS), a statutory agency under the Ministry of Commerce, is responsible for standards and setting up technical committees for standards deliberation. The private sector and academics usually also participate in the technical committees.
Objectives on technical standards	India's draft Standards National Action Plan (2022) identifies AI as part of a group of technologies that will drive future standardisation efforts. Other technologies include big data, the internet of things and quantum computing. The plan recognises the need to increase expert participation in national delegations to the ISO and IEC, although digital technologies have been designated as a 'medium priority' in BIS's action plan.[179]
Objectives on the (global) governance of AI	The draft Standards National Action Plan refers to emerging technologies, including AI / machine learning (ML), as an emerging national priority but doesn't articulate specific objectives. However, India has signed on to statements that underscore the importance of standards-setting at the Quad, in particular the Quad International Standards Cooperation Network.[180] This signals a diplomatic commitment to standards-setting for critical technology.
Preferred forums for international engagement	India prefers to engage through UN bodies and traditional SDOs such as the ISO and ITU. India has funded an ITU office in India in 2023[181] and specifically mentioned its relevance in the setting of high-tech standards in areas such as 6G.[182] As a member of the Quad, India signed on to the Principles on Critical and Emerging Technology Standards (2023).[183] Bilaterally, the US and EU are important partners for India. In 2022, India and the US introduced the US–India Critical and Emerging Technologies (iCET) initiative as an institutional mechanism 'to build open, accessible, secure, and resilient technology ecosystems and value chains, based on mutual confidence and trust, which reinforce our shared values and democratic institutions'.[184] With the EU, India established a trade and technology council in 2023 to coordinate key challenges in trade, trusted technology and security. Cooperation on trustworthy AI is one of the topics.[185]

Japan

National interests and priorities	Japan aims to realise 'Society 5.0' – a resilient society through the fusion of cyberspace and physical space - and contribute to the UN Sustainable Development Goals based on three principles: dignity for people, diversity and sustainability.[186] Japan has identified five strategic objectives that underpin the three principles: human resources, industrial competitiveness, technology systems, international cooperation, and dealing with imminent crises.[187]
Governance model for technology	Government leads standards development through the Japanese Industrial Standards Committee (JISC) of the Ministry of Economy, Trade and Industry (METI). However, in line with the government's 'agile governance' approach, the guidance documents to support AI principles implementation were prepared through multistakeholder dialogues.[188]
Objectives on technical standards	METI's JISC revises and introduces standards in response to technological advances. The standards stipulate the criteria for data, mineral or industrial products and services in Japan, including their quality, performance and test methods.
Objectives on the (global) governance of AI	Japan has prioritised addressing the global AI divide and building collaborations with international organisations such as the G20, G7 and OECD to do so. On data sharing, it has proposed collaborations to design global data governance rules to promote data free-flow with trust.[189]
Preferred forums for international engagement	Japan has identified the GPAI as a practical international framework initiative to align with global standards for AI and data governance. As a member of the Quad, it signed on to the Principles on Critical and Emerging Technology Standards to promote the use of AI in line with democratic norms and values. At the 2023 G7 Digital and Tech Ministers' Meeting, Japan (then G7 President) and other G7 economies extended support:[190] • for the development, adoption and promotion of international technical standards in SDOs through sector-led multisectoral processes • to SMEs, academia and start-ups to participate in SDOs.

Singapore

National interests and priorities	In 2018, Singapore introduced 'Smart Nation: the way forward'—a plan to prepare Singapore for a new disruptive phase of development with AI/ML at its centre.[191] It's primarily focused on domestic transformation 'where a Digital Government, Digital Economy and Digital Society harness technology to effect transformation in health, transport, urban living, government services and businesses.'[192] In that context, Singapore launched the country's model AI Governance Framework in 2019[193] to develop principles, frameworks and recommendations on AI ethics and governance. Singapore's Ministry for Communications and Information has announced the launch of the Artificial Intelligence (AI) Verify Foundation to harness the collective power and contributions of the global open-source community to develop AI testing tools for the responsible use of AI.[194] The foundation focuses on promoting best practices and standards for AI.
Governance model for technology	Singapore follows a light-touch regulatory approach towards AI standards, encouraging industry to voluntarily adopt responsible AI with detailed government guidance. The AI Governance Framework has been developed with inputs from more than 60 national and international companies of different sizes from different industry sectors.
Objectives on technical standards	Singapore aims to be a leader in developing and deploying scalable, impactful AI solutions in key sectors of high value and relevance to its citizens and businesses by 2030.[195]
Objectives on (global) governance of AI	Singapore's National AI Strategy 2023 makes reference to Singapore's international reputation as an early adopter and pragmatic partner. The government further commits to 'contribute actively to international discourse on AI governance, to raise capacity, share best practices, and shape rules around AI, together with the international community'.[196]
Preferred forums for international engagement	Singapore has a multipronged approach to international engagements. It follows UN discussion intensely and is often the initiator of regional coordination within ASEAN. Singapore is also active in various multistakeholder platforms, such as the GPAI and the World Economic Forum AI Governance Alliance, and has been admitted to the UN Advisory Body on AI.[197] Furthermore, Singapore has intensified bilateral conversations with the US and China. Pursuant to the US–Singapore Critical and Emerging Technology Dialogue,[198] Singapore will also start a digital policy dialogue with China in 2024.[199]

ASEAN

Interests and priorities	ASEAN's priorities in emerging and critical technology are to drive economic growth through the digital economy and harmonise standards across all ASEAN states.[200] Ultimately, ASEAN hopes to leverage new technologies, including AI, to support economic growth, administrative efficiency and social uplift.[201]
Governance model for technology	ASEAN doesn't have a single governance approach to technology. Its main role is to coordinate policy actions among its member states to ensure coherence and coordination in support of, for instance, the ASEAN Digital Masterplan 2035. Specific issues of shared concern are addressed through sectoral frameworks, such as frameworks for digital data governance,[202] data management[203] and cybersecurity.
Objectives on technical standards for AI	The ASEAN Digital Trade Standards Working Group is the main platform for coordinating discussions on standards-setting in the context of addressing technical barriers to trade. Its 2021–2025 work plan looks at six items: e-commerce; e-invoicing; e-payments; last mile delivery; digital identity and e-signatures; and cybersecurity.[204] On those topics, ASEAN and Australia are working together under the Digital Trade Standards Initiative to support national bodies with research, analyses and workshops.[205]
Objectives on (global) governance of AI	One action item from the ASEAN Digital Masterplan suggests the 'development and adoption of a regional policy to deliver best practice guidance on AI governance and ethics'. This was delivered with the ASEAN Guide on AI Governance and Ethics, which was endorsed in February 2024. The guide recommends that ASEAN should set up a regional working group on AI governance and is built on existing use-cases of entities such as Gojek, Ucare.ai and the Singapore Government. The purpose is predominantly to help and empower companies, organisations and governments to design, develop and deploy traditional AI systems responsibly and increase users' trust in AI.[206] ASEAN doesn't have a formal plan to inform and engage with global governance initiatives.
Preferred forums for international engagement	The ASEAN Digital Ministers' Meeting is the primary forum for regional discussions on emerging technology, cybersecurity and digital standards.

Key takeaways

- Countries have different starting positions on the governance of emerging technologies, including AI. They range from a predominantly free-market and more industry-driven approach, as in the US, to state-directed approaches, as in China. Others, such as the EU, take a middle ground based on regulatory action on individual rights and market competition. At the same time, they all rely—to a lesser or greater extent—on private-sector consultations and co-development.
- There are shared objectives, if not common approaches. Each of the countries reviewed is seeking a combination of maintaining or acquiring a technological advantage through R&D (technological security); securing technological sovereignty and preventing misuse (national security); building future-proof jobs, businesses and local competitive AI industry (economic security); and protecting cultural identities, social norms and cohesion and personal data (social security). Of course, their definitions of, for example, 'national security', 'economic security' and 'technological sovereignty' vary considerably.
- Countries have different preferred forums for international engagement. China, Southeast Asian and Pacific governments prefer multilateral, government-to-government and UN-based forums to advocate for their interests. On the other hand, the US and its closest partners have invested significantly in smaller and minilateral groupings within their 'trusted geographies' to develop common positions. The EU is predominantly preoccupied with ensuring the singularity of the internal European market. The extraterritorial effects of pieces of EU legislation (such as the General Data Protection Regulation) have been welcome side effects.
- This overview highlights the fragile nature of the techdiplomacy landscape in the Indo-Pacific. In the absence of a major Indo-Pacific platform to discuss AI, governance and standardisation (the ASEAN Digital Masterplan remains at an early stage of maturity and covers only a part of the region), individual countries have to selectively deploy their resources and attentions and carefully select partners to work with on particular areas of concern or interest. Within countries, the overview also shows the need for structured exchanges between the various bodies of government, NSBs and industry communities to instil awareness and build maturity in understandings of national security, technology and industrial-development policies.

Chapter 6: Recommendations for informing and building an agenda for Indo-Pacific AI techdiplomacy

This playbook has examined the complex ecosystem of global AI governance, the role of technical standards, the processes of standards negotiations, important 'movers and shakers', and the current positions of various Indo-Pacific actors.

Capabilities for AI techdiplomacy in the Indo-Pacific are currently limited, even though AI will inevitably affect the region's socio-economic, political and security domains significantly. While China, the EU and the US are leading the way in formulating the future parameters of global governance and technical standards for AI, their different approaches may pull different nations in the region into different 'spheres of preference'.

A primary step in preventing a potential splintering of AI governance is to develop a region-specific agenda, engagement and negotiation plan. With that in mind, we outline eight recommendations and steps to help inform and build an Indo-Pacific agenda for AI techdiplomacy.

1: Mobilise a national or regional techdiplomacy community

A first step for governments and national standards bodies in the region should be to mobilise a multistakeholder community of interest—a national or regional AI technology forum[207]. This would allow different stakeholder groups, who all operate within their own remits and mandates, to learn from one another. It would enable the correlation of principles of responsible governance with regulatory initiatives and the development of technical standards.

Given the agile and innovative nature of the technology and its applications, stakeholder views and concerns are in flux, too, and evolve relatively quickly. It's important for governments and NSBs to stay abreast of changes. At a minimum, at the national level, the community ought to understand—and recognise—the variety in national-level touchpoints when it comes to setting global rules, principles and standards, and who plays which role in that debate.

2: Define what the role and impact of AI technology should and shouldn't be

It's imperative for each country to now define what it wants AI to deliver to its society and economy, where it's comfortable introducing AI technologies, and where it doesn't want AI to be applied. Policymakers should consider whom they want to be driving AI technologies, under which types of governance regimes, and whom they entrust with setting rules and standards. In the few situations where that has happened, such as in Australia with the AI Standards Roadmap, and where the product can rely on broad community support, such road maps helpfully inform national positions and subsequent (international) engagements.

3: Catalogue indigenous strengths and capabilities

A next step would be for individual nations to take stock of their indigenous national capabilities in AI technologies. Positions on the future role of technology, and the needs and requirements of (global) governance, are informed by one's relative strength and competitiveness. Consulting ASPI's *Critical Technology Tracker*—which measures high-impact research and the flow of global technology talent and reveals where countries, universities, companies and national labs around the world have a competitive advantage across 64 technologies—is an example of an exercise that's compelled many countries to critically assess and re-evaluate their domestic strengths and capabilities in AI and other critical technologies.[208]

Further considerations include reviews of:

- the commercial success of start-ups, scale-ups and established industries in terms of market size, employment or attracting investments
- policy and regulatory influence, for instance through the introduction of innovative and fit-for-purpose policy concepts and international presence and engagement
- the influence and credibility of non-government entities and civil-society actors in terms of advocacy.

4: Determine the preferred and most effective means of AI governance

A fourth step is to determine which instrument of governance—domestically, regionally and globally—best suits the needs of society and the capabilities of government and industry to monitor, verify and enforce. Following the Singapore model of AI Verify, this could well be a mix of methods and instruments initiated elsewhere that can then be tailored to the local context. Preferred instruments will also change over time with the increasing domestic maturity of and developments in technology and social acceptance. However, the baseline will have to be grounded in common agreed technical standards and shared principles for the responsible development and use of AI technologies.

5: Prioritise platforms for international engagement

The governance of critical technologies, and AI in particular, is necessarily an international effort of coordination, cooperation and alignment on minimum principles and standards. This is a consequence of the global nature of the market and the global nature of the technology. Subject to each nation's requirements, opportunities, strengths and capabilities, as well as existing international partnerships, the country should be able to select and prioritise those international platforms that are expected to produce results that are most conducive to its interests in AI and global governance—or the forums that it prefers to see emerge as leading groups.

It's unlikely that most Indo-Pacific nations will be able to follow, monitor and participate in every initiative, so prioritisation is inevitable. That may provide a stimulus for greater regional coordination, such as through the Quad Standards Coordination Group, or with ASEAN, the South Asian Association for Regional Cooperation (SAARC) and the East Asia Summit.

6: Establish ambassadorial or sherpa-type roles for standards negotiations

To mobilise national multistakeholder communities and to encourage nations to strategise their international engagements in technical standards-setting, it's worth considering establishing an ambassadorial or sherpa-type role. This would be a senior-level person who can give direction to a whole-of-government or ideally a whole-of-economy effort, and who can mobilise public-sector and industry expertise. Most likely, this person would have a coordinating rather than a commanding mandate and would play a public-facing role. This seems to be an effective and accepted practice originating out of the G20. It's also being applied to, for instance, the coordination of national multistakeholder delegations attending the four-yearly ITU plenipotentiary meetings and participating in international conferences such as the Global Conference on Cyberspace and the Summit on Responsible AI in the Military Domain.

7: Foster accessibility and transparency of standards

At the moment, the bulk of technical standards and the underpinning proceedings are exclusive—they lack openness and transparency. For instance, lists of participants, minutes of proceedings and outcome documents aren't accessible in the public domain. For many institutions in emerging economies, a paid-access arrangement for agreed international standards is a barrier to access and adoption.

At present, most standards critical to AI—such as those published by SDOs and used by private companies—are confidential or behind paywalls. That inhibits independent research, verification, openness and transparency. The IEEE has taken a step to make selected standards available free of charge to encourage the 'adoption and use of standards that contribute to advancing technology for humanity in key areas'.[209] Diplomatic efforts should be directed to ensuring that this practice is followed at greater scale and by all standards organisations.

8: Support and grow diversity of geographies, gender and groups

Finally, it's important to ensure that techdiplomacy platforms have diversity in their representation of geographies, gender and type of stakeholder groups (government, industry, academia, civil society, technical community). To ensure that those who need access can have access, examples can be drawn from the cybersecurity and internet communities.

In recent years, various initiatives have grown that, among other things, support greater participation of women from underrepresented economies in UN-level discussion. Examples include:

- The Women in Cyber Fellowship.[210] An AI version could target participation in negotiations around the UN Global Digital Compact.
- Technical, policy and community engagement fellowships that encourage newcomer individuals and organisations to become part of the community. In the internet technical domain, such fellowships are offered by organisations such as the Asia Pacific Network Information Centre, the Internet Society and the Internet Corporation for Assigned Names and Numbers)
- Initiatives such as Let's Talk Cyber[211] which creates a platform to rally multistakeholder conversations with more diverse geographical representation in the margins of government-led negotiations. Events such as India's Global Technology Summit, Australia's Sydney Dialogue[212] and Singapore's International Cyber Week or Quad events also play a mobilising role.

Conclusion

This concludes our playbook for negotiating technical standards for AI. We hope that we've given policymakers and technologists in the Indo-Pacific greater insights into the world of standards-making and also amplified the need for Indo-Pacific stakeholders, from advanced, emerging and developing economies, to be represented in this space. This is particularly relevant, since AI is expected to have such a transformative impact on our social, economic and political lives.

That means that the role of government remains very important, and that policymakers should seek opportunities to become and remain involved. It is not to say, however, that government needs to take up a lead role *per se*.

The pluriform nature of the technology governance landscape and of standards-setting involves many actors and stakeholders, each carrying their values and interests and advocating for their positions. This includes the academic who prepares research for a GPAI working group; the company participating in ISO Subcommittee 42; the civil society organisation advocating for human rights guarantees; and the AI start-up experimenting with new applications.

They all play a *diplomatic role* in shaping agendas, setting boundaries and direction, and moving standards- and rules-making processes forward.

It's essential that this entire multistakeholder community is sufficiently equipped with knowledge and skills to engage in negotiations on technical standards as part of the 'big push for AI governance'.

We hope that this playbook helps to advance this cause.

Glossary

Artificial intelligence (AI): a technology that involves the computerised capability of an entity or a machine to exhibit behaviours that resemble human intelligence. based on robust datasets and focused on solving problems.[213]

AI governance: the system of rules, practices, processes and tools across the life cycle of AI systems: pre-design, design, development, evaluation, testing, deployment, use, sales, procurement, operations and decommissioning.

AI regulation: the collection of laws, regulations and other legal instruments through which government can enforce compliance by AI developers, manufacturers, providers and users with codified rules, laws and standards.

Critical technologies: emerging and/or disruptive technologies that can significantly affect the national security, economic prosperity and social cohesion of states.[214]

Disruptive technologies: technologies capable of fundamentally changing the rules and business models of a market or society.[215]

Emerging technologies: new and innovative technologies being developed or recently introduced into the market that aren't yet fully established.[216]

Frontier AI: models of AI that surpass previously existing capabilities and have the potential to have dangerous consequences for human and global security.[217]

Foundation AI models: models trained on broad datasets with a high degree of self-supervision and requiring large amounts of data and great computational power; they're built to form the basis for other, often user-facing, applications.[218]

Generative AI: models or algorithms (such as ChatGPT) that can create new content, including audio, code, images, text, simulations and videos.[219]

Interoperability: the ability of different systems, devices or applications, developed by different people and companies and under different jurisdictions, to connect and operate effectively with each other; AI standards frequently aim to enhance interoperability.

Large language model (LLM): a form of machine learning that can perform natural-language processing tasks, such as answering questions and translating text; the LLM underpinning Google Translate is an example.[220]

Machine learning (ML): A subset of AI that involves developing models or algorithms that can learn and make decisions on their own, based on data.

Standards-developing organisation (SDO): a recognised national, regional or global organisation (such as the ISO or the Bureau of Indian Standards) focused on developing, publishing and disseminating technical standards to meet the needs of an industry or field.[221]

Technical standards: agreed requirements that specify how a particular technology product or service should be designed and/or perform; in AI, the standards could relate to aspects such as safety, interoperability, data privacy and reliability.

Notes

1 Various authors from OpenAI, 'Language models are few-shot learners', 22 July 2020, online.

2 AI is driving business to go even further with digitisation and move towards hyper-automation. Thus far, the bulk of digitisation has involved digitising and aiding manual processes. We're now looking at radical transformations in human–machine teaming, allowing companies to rely on machines to deliver customer service and personalised content and services, and to be more specific in forecasting, performance and risk management. With inputs from ChatGPT as well as Chakri Gottemukkala, 'The future of AI: three ways AI will shape business transformation', *Forbes*, 15 March 2024, online.
The IMF estimates that, globally, 40% of jobs will be affected by AI, and in advanced economies even 60%. See Mauro Cazzaniga et al., 'Gen-AI: artificial intelligence and the future of work', staff discussion note, International Monetary Fund, 14 January 2024, online. The automation of routine tasks and the augmentation of creative and other human tasks are changing the character and skill sets of workforces as well as education needs across societies.
AI applications enable near real-time monitoring of the movement of ice in the Antarctic; measurements of deforestation in remote and inaccessible areas and the amount of carbon stored in forests; predictions of longer term weather patterns, which allow vulnerable communities to prepare and adapt; and assistance to manufacturers to reduce waste and emissions and integrate renewable energy sources. With inputs from ChatGPT and Vittoria Masterson, '9 ways AI is helping tackle climate change', World Economic Forum, 21 February 2024, online.
In the health sector, AI helps medical professionals to interpret images, test results and other data more quickly and effectively, enabling them to offer patients earlier detection and more effective and personalised cures, drugs and medications. With inputs from ChatGPT and Lael Brainard, Neera Tanden, Arati Prabhakar, 'Delivering on the promise of AI to improve health outcomes', The White House, 14 December 2023, online.

3 Generative AI can generate text, images and even music that closely resembles original works. It might replicate copyrighted material. AI-powered content can also be misused to create counterfeit products or plagiarised content, or it can generate content on the basis of data that wasn't licensed for use. With inputs from ChatGPT and Gil Appel, Juliana Neelbauer, David Schweidel, 'Generative AI has an intellectual property problem', *Harvard Business Review*, 7 April 2023, online.
AI is also known to produce outputs on the basis of its training data and algorithms. When those are skewed, the outputs of models and applications are consequently also skewed. That can happen, for instance, when banks are assessing loans and mortgages, or when police are assessing high-crime areas and suspect individuals. With inputs from ChatGPT and Reva Schwarts et al., *Towards a standard for identifying and managing bias in artificial intelligence*, special publication 1270, National Institute of Standards and Technology (NIST), March 2022, online.

4 Olivier Salvadi, Jon Whittle, 'AI pioneer Geoffrey Hinton says AI is a new form of intelligence unlike our own. Have we been getting it wrong this whole time?', *The Conversation*, 4 May 2023, online.

5 'Statement on AI risk', Center for AI Safety, no date, online.

6 Such statements typically commit companies to uphold principles such as fairness and equity; transparency and explainability; privacy and data protection; accountability and governance; and robustness and reliability.

7 See the seminal work of Harvard scholars Roger Fisher, William Ury and Bruce Patton on negotiations. They codified the practice of distinguishing between negotiating parties' positions, interests and values in *Getting to YES: negotiating agreement without giving in*, Penguin Books, New York, 1991, online. See also the work of the Processes of International Negotiation (PIN) Program network, a group of scholars and practitioners that encourages and organises research on a broad spectrum of topics related to international negotiation as seen as a process, online.

8 Department of Foreign Affairs and Trade (DFAT), *Australia's International Cyber and Critical Technology Strategy, Australian Government*, 2021, 78–79, online.

9 Rajeswari Pillai Rajagopalan, 'The growing tech focus of the Quad', *The Diplomat*, 8 July 2022, online; 'Quad Leaders' Summit fact sheet', The White House, Washington DC, 20 May 2023, online.

10 DFAT, 'Cyber affairs and critical technology: India partnership', Australian Government, 2024, online.

11 Ian Levy, 'So long and thanks for all the bits'. Blog. UK National Cyber Security Centre. 27 October 2022, online.

12 US Geological Survey, 'Standards and specifications—what exactly are they?', US Government, 2024, online.

13 See, for instance, the work of Laura DeNardis: 'Protocol politics: the globalization of internet governance' (2009), 'The global war for internet governance' (2014) and 'The internet in everything: freedom and security in a world with no off switch' (2020).

14 AI fringe, 'Standards for responsible AI—Day 2', *YouTube*, 1 November 2023, online; *Global technology governance: a multistakeholder approach*, White Paper, World Economic Forum, October 2019, online.

15 'Standards in our world', International Organization for Standardization (ISO), no date, online.

16 Tim Ruhlig, 'Transatlantic tech de-risking from China: the case of technical standards-setting', testimony before the US–China Economic Security Review Commission, 15 June 2023, online.

17 Peter Cihon, *Standards for AI governance: international standards to enable global coordination in AI research & development*, Future of Humanity Institute, University of Oxford, April 2019, online.
18 Cihon, *Standards for AI governance: international standards to enable global coordination in AI research & development*.
19 Cihon, *Standards for AI governance: international standards to enable global coordination in AI research & development*.
20 'What are standards?', NBN, no date, online.
21 HTTPS = hypertext transfer protocol secure; DNSSEC = domain name system security extensions; TLS = transport layer security.
22 Emily Jones, 'Digital disruption: artificial intelligence and international trade policy', *Oxford Review of Economic Policy*, Spring 2023, 39(1):70–84, online; Also, for example, India's Sensitive Personal Data Rules incorporate the international standard ISO/IEC 27001 on 'Information Technology—Security Techniques—Information Security Management System' as an Indian Standard for 'reasonable security practices'.
23 David Berlind, 'The making of de facto standards', *ZD Net*, 11 April 2002, online.
24 Simon den Uijl, 'The emergence of de-facto standards', PhD thesis, Erasmus University, Rotterdam, 2015, 219, online.
25 'Huawei agrees long-term patent deal with Ericsson despite Western curbs, *Financial Times*, 25 August 2023, online.
26 Hildegunn Kyvik Nordås, *Services domestic regulation: envisioning next generation technical standards principles*. US-Support for Economic Growth in Asia. Report for Asia-Pacific Economic Cooperation. March 2024, online.
27 'IPR policy', European Telecommunications Standards Institute (ETSI), no date, online.
28 Shu-Hao Chang, 'Technical trends of artificial intelligence in standard essential patents', *Data Technologies and Applications*, 55(1):97–117.
29 Tim Ruhlig, *China, Europe and the new power competition over technical standards*, Swedish institute of International Affairs, 2021, online.
30 'IPR policy', ETSI.
31 John Cassels, 'What is FRAND', *fieldfisher*, 23 August 2013, online.
32 Bjorn Fägersten, Tim Rühlig, *China's standard power and its geopolitical implications for Europe*, brief no. 2, Utrikespolitiska Instututet, March 2019, online.
33 'Technical Barriers to Trade Agreement', World Trade Organization (WTO), no date, online; 'International standards "and private standards"', ISO, February 2010, online.
34 DFAT, 'Technical barriers to trade', Australian Government, no date, online.
35 'Regional Comprehensive Economic Partnership Agreement', November 2020, online.
36 'Principles for the development of international standards, guides and recommendations', WTO, 2000, online.
37 'New specific trade concerns', WTO, March 2022, online.
38 'How to build cyber resilience', ISO, February 2023, online.
39 'ISO 27001—Information security management', ISO, 2013, online
40 Tim McGarr, 'Safety, security, and resilience in trustworthy AI', *AI Standards Hub*, no date, online.
41 Sabrina Weithmann, Susann Luedtke, 'Evaluating the impact of deviating technical standards on business processes, trade, and innovation', *Journal of Standardisation*, 8 June 2023, online.
42 'Tech industry calls for AI-friendly rules in Australia', *Digital Watch*, 28 August 2023, online.
43 'Safe, secure, and trustworthy development and use of artificial intelligence', executive order, The White House, 1 November 2023, online.
44 'G8 statement on information and communication technologies', University of Toronto, 2023, online.
45 Narendra Modi, keynote address at The Sydney Dialogue, 18 November 2021, online.
46 Ministry of Electronics and Information Technology, 'Proposed Digital India Act', Indian Government, 2023, online; Simon Sharwood, 'India teases AI Plan to catalyse the next generation of the internet, *The Register*, 8 March 2023, online.
47 'What is AI Verify?', AI Verify Foundation, no date, online; Personal Data Protection Commission of Singapore, 'Singapore's approach to AI governance', 2020, online.
48 Jake Evans, 'Artificial intelligence technologies could be classified by risk, as government consults on AI regulation', *ABC News*, 1 June 2023, online.
49 Matt Sheehan, 'China's AI regulations and how they get made', Carnegie Endowment for International Peace, 10 July 2023, online; 'Basic safety requirements for generative artificial intelligence services' (生成式人工智能服务安全基本要求), translation, Georgetown Center for Security and Emerging Technology, 4 April 2024, online.
50 'Fact sheet: President Biden issues Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence', The White House, Washington DC, 30 October 2023, online.
51 'International community must urgently confront new reality of generative, artificial intelligence, speakers stress as Security Council debates risks, rewards', news release, UN, 18 July 2023, online.
52 'Seizing the opportunities of safe, secure and trustworthy artificial intelligence systems for sustainable development', Resolution A/79/L49, UN General Assembly, 11 March 2024, online.

53 Cade Metz, 'The dark secret at the heart of AI,', *MIT Technology Review*, 11 April 2017, online; 'Artificial intelligence and robotics', European Parliament, 2019, online.
54 Tobias Vestner, Juliette François-Blouin, 'Globalizing responsible AI in the military domain by the REAIM Summit', *Just Security*, 13 March 2023, online.
55 See Paul Sharre, *Four battlegrounds: power in the Age of Artificial Intelligence*, WW Norton, 2023.
56 'National Artificial Intelligence Research Resource Task Force', The White House, Washington DC, 5 December 2022, online.
57 For an account of the role of rules, norms and principles, see Bart Hogeveen, *The UN norms of responsible state behaviour in cyberspace: guidance on implementation for member states of ASEAN*, Australian Strategic Policy Institute (ASPI), Canberra, 22 March 2022, online.
58 'International community must urgently confront new reality of generative, artificial intelligence, speakers stress as Security Council debates risks, rewards', news release, UN, 18 July 2023, online.
59 Camino Kavanagh, *New Tech, New Threats, and New Governance Challenges: An Opportunity to Craft Smarter Responses?* Carnegie Endowment, August 2019, online; Ashley Deeds, *A New Tool for Tech Companies: International Law*. Lawfare, 30 May 2019, online.
60 'Responsible AI', Microsoft, 2024, online.
61 'Our principles', Google AI, no date, online.
62 'AI ethics', IBM, no date, online.
63 'Principled artificial intelligence', Harvard Cyberlaw Clinic, 2020, online.
64 Mariarosaria Taddeo, Luciano Floridi. 'How AI can be a force for good', *Social Science Research Network*, 17 April 2015, online.
65 'Fact sheet: Biden–Harris administration secures voluntary commitments from leading artificial intelligence companies to manage the risks posed by AI', The White House, Washington DC, 21 July 2023, online.
66 The drama involving ChatGPT's owner, OpenAI, is a case in point. The board, concerned with the company's mission of 'cautious AI', believed that the CEO was moving too fast and decided to fire him. As the local tech community and employees of OpenAI objected to that move, and Microsoft decided to hire the ousted CEO, the board was forced to turn back its decision and resign itself. Competitiveness and commercial interests trumped the mission of cautious AI and AI for public good. Eugenia Lostri, Alan Z Rozenshtein, Chinmayi Sharma, 'The chaos at OpenAI is a death knell for AI self-regulation', *Lawfare*, 28 November 2023, online.
67 Suzannah Auyong, 'AI and the rule of law', in Theo Lynn, Chris Reed, Karl Branting (eds), *The law of artificial intelligence and smart machines: understanding AI and the legal impact*, Wiley, 2022, online; Brent Mittelstadt, 'AI ethics: a view from Europe', *Nature Machine Intelligence*, 2019, 1: 447–50, online; 'What is the problem with "ethical AI"? An Indian perspective', *CyberBRICS Project*, 17 July 2019, online.
68 'Safe, secure, and trustworthy development and use of artificial intelligence', executive order, The White House, Washington DC, 1 November 2023, online.
69 See, for instance, Global Cyber Security Capacity Centre, 'Cybersecurity capacity maturity model for nations', Oxford Martin School, University of Oxford, 2021, online.
70 'AI Act: a step closer to the first rules on artificial intelligence', media release, European Parliament, 11 May 2023, online.
71 Huon Curtis, Bart Hogeveen, Jocelinn Kang, Huong Le Thu, Rajeswari Pillai Rajagopalan and Trisha Ray, *Digital Southeast Asia. Opportunities for Australia–India cooperation to support the region in the post-Covid-19 context.* Australian Strategic Policy Institute. February 2022, page 15, online.
72 Ed Husic, 'Action to help ensure AI is safe and responsible', media release, Minister for Industry, Australian Government, 17 January 2024, online; Nick Bonyhady, 'Business is about to get a say on AI rules', *Australian Financial Review*, 19 April 2024, online.
73 Alessio Tartaro, Adam Leon Smith, Patricia Shaw, 'Assessing the impact of regulations and standards on innovation in the field of AI', *arXiv preprint* arXiv:2302.04110, 2023, online; Department for Business and Trade, Department for Business, Energy and Industrial Strategy, *Regulation for the Fourth Industrial Revolution*, UK Government, 11 June 2019, online; Brigitte Krogman, Rainer Spittel, 'Regulatory reform and innovation', Organisation for Economic Co-operation and Development (OECD), 2018, online.
74 'Ethics of artificial intelligence in the context of the Fourth Industrial Revolution', OECD, 2018.
75 Interview with Singapore Infocomm Media Development Authority, 18 November 2022.
76 'What is AI Verify?', AI Verify Foundation, no date, online; interview IMDA, 18 November 2022.
77 See, for instance: World Trade Organisation, 'Annex 4(b) Agreement on Government Procurement'. Amended on 30 March 2012, online.
78 'NATO starts work on artificial intelligence certification standard', North Atlantic Treaty Organization (NATO), 8 February 2023, online.
79 We also opt to look at the international governance of AI through the prism of a 'regime complex', in which elements of international law, political declarations and principles, in conjunction with domestic legislation, industry practices and universal technical standards, amount to a global ecosystem of governance. See Laura Gómez-Mera, 'International regime complexity', in Renée Marlin-Bennett (ed.), *Oxford Research Encyclopedia of International Studies*, Oxford University Press, 31 August 2021, online.
80 'GPAI terms of reference', Global Partnership on Artificial Intelligence (GPAI), no date, online.
81 Center for International Relations and Sustainable Development, 'Going nuclear', *Horizons*, Summer 2023, issue 24, online.
82 'G7 Hiroshima AI Process: G7 digital & tech ministers' statement', *Politico Europe*, 7 September 2023, online.

83 'REAIM 2023: Call to action', Netherlands Government, 16 February 2023, online.
84 'Our common agenda: Policy brief 9: A new agenda for peace', UN, July 2023, online.
85 Office of the Secretary-General's Envoy on Technology, 'Global Digital Compact', UN, no date, online.
86 'UN Secretary-General launches AI Advisory Body on risks, opportunities, and international governance of artificial intelligence', media release, UN, 25 October 2023, online.
87 Laurie Clarke, Annabelle Dickson, Cristina Gallardo, 'Rishi Sunak: UK wants to lead the world on AI. The world ain't listening', *Politico*, 5 June 2023, online; Department for Science, Innovation and Technology et al., 'Chair's summary of the AI Safety Summit 2023, Bletchley Park', UK Government, 2 November 2023, online.
88 'Australia–India–Japan–US principles in practice', Track 1.5 strategic dialogue, ASPI, Canberra, 26 July 2023.
89 Penny Wong, 'National Press Club Address, Australian interests in a regional balance of power'. 17 April 2023, online.
90 'ISO Code of Conduct', ISO, 23 February 2023, online; 'IETF guidelines for conduct', Internet Engineering Task Force (IETF), March 2014, online.
91 These definitions are compiled from ISO, AI standards hubs and Standards Australia.
92 'Standards by ISO/IEC JTC 1/SC 42: Artificial intelligence', ISO, 2024, online.
93 'PP-22 closing press release', International Telecommunication Union (ITU), 14 October 2022, online.
94 'Standards in our world', ISO, no date, online.
95 Standards Australia, *An Artificial Intelligence Standards Roadmap: making Australia's voice heard*, Standards Australia, no date, online.
96 'About IEEE Standards Association', IEEE Standards Association, no date, online.
97 'Introduction to the IETF', IETF, no date, online.
98 Steven Levy, 'Huawei, 5G, and the man who conquered noise', *Wired*, 16 November 2020, online.
99 See, for instance, Sebastien Bubeck et al., 'Sparks of artificial general intelligence: early experiments with GPT-4', *Arxiv*, Cornell University, 13 April 2023, online.
100 This case study was written in consultation with Microsoft.
101 Satya Nadella, 'Humans and AI can work together to solve society's challenges', *Slate*, 29 June 2016, online.
102 Microsoft, 'Developing Microsoft's Responsible AI Standard', *YouTube*, 20 May 2020, online.
103 'AI Risk Management Framework', NIST, 2024, online.
104 *Governing AI: a blueprint for the future*, Microsoft, 25 May 2023, online.
105 *Governing AI: a blueprint for the future*.
106 'Ensure the internet remains a foundation for a sustainable future', Internet Society, 22 January 2009, online.
107 Categorisation and classification by one of the authors.
108 'Huawei's "New IP" proposal—frequently asked questions', Internet Society, 22 February 2022, online.
109 'Interpret China: China Academy of Information and Communications Technology (CAICT)', Center for Strategic and International Studies, 1 September 2022, online.
110 Huawei Technologies Co. Ltd (China), China Mobile Communications Corporation, China Unicom, Ministry of Industry and Information Technology (MIIT), '"New IP, shaping future network": Proposal to initiate the discussion of strategy transformation for ITU-T', proposal TSAG-C83, September 2019.
111 See, for instance, Mark Montgomery, Theo Lebryk, 'China's dystopian "New IP" plans shows need for renewed US commitment to internet governance', *Just Security*, 13 April 2021, online; Anna Gross, Madhumita Murgia, 'China and Huawei propose reinvention of the internet', *Financial Times*, 27 March 2020, online; Munish Sharma, 'New internet protocol: redesigning the internet with Chinese characteristics', *Indian Defence Review*, 12 November 2020, online.
112 Office of the Chief Technology Officer, 'New IP', ICANN, 27 October 2020, online; RIPE NCC, 'Response to "New IP, shaping future network" proposal', February 2020, online; Hascall Scharp, Olaf Kolkman, 'Discussion paper: An analysis of the "New IP" proposal to the ITU-T', Internet Society, 24 April 2020, online.
113 Hunter Dorwart, 'New IP proposal to ITU-T would give governments more control over the internet—here's why that is a problem', *TIA Online*, Telecommunications Industry Association, no date, online.
114 Montgomery & Lebryk, 'China's dystopian "New IP" plan shows need for renewed US commitment to internet governance'.
115 Paul Meerts, *Diplomatic negotiation: essence and evolution*, Clingendael Institute, 2015, 202.
116 'ISO/IEC JTC 1/SC 42: Artificial intelligence', ISO, 2024, online.
117 ISO, 'JTC 1, Sub-committee 42 Artificial intelligence', May 2023, online (accessed April 2024).
118 'Getting started kit for ISO committee managers', ISO, 2023, online; 'My ISO job. What delegates and experts need to know', ISO, 2018, online.
119 'My ISO job. What delegates and experts need to know'.
120 'JTC 1, Sub-committee 42 Artificial intelligence'.
121 'ITU-T focus groups', ITU, no date, online.
122 'Focus groups: establishment and working procedures', ITU, no date, online.
123 'Focus groups: establishment and working procedures'.

124 'Active PARs', IEEE Standards Association, 2024, online.
125 'What is IEC vs IEEE standard?', *China Gauges*, online.
126 'Top 5 country visual snapshot', *Critical Technology Tracker*, ASPI, Canberra, 22 September 2023, online.
127 'Mandate of the International Panel on Artificial Intelligence', Canadian Government, 6 December 2018, online.
128 Secretary-General, 'Remarks announcing the High-Level Advisory Body on Artificial Intelligence', UN, 26 October 2023, online.
129 Advisory Body on Artificial Intelligence, *Interim report: Governing AI for humanity*, UN, December 2023, online; 'Global Digital Compact: zero draft'. 1 April 2024, online.
130 China's Ministry of Foreign Affairs, 'Global AI Governance Initiative', Communique, 20 October 2023, online.
131 See: Danielle Cave, Fergus Ryan and Vicky Xu, 'Mapping more of China's tech giants: AI and surveillance'. Australian Strategic Policy Institute, November 2019, online.
132 Bill Drexel, Hannah Kelley. 'How China plans to win the future', *Politico*, 30 November 2023, online; Niva Yau, Dirk van der Kley, 'China's global network of vocational colleges to train the world', *The Diplomat*, 11 November 2021, online.
133 'What is tech diplomacy? Experts explain', World Economic Forum, 23 February 2023, online.
134 'Critical Technology Standards Metric', Brookings Institution, no date, online.
135 Graham Webster, Rogier Creemers, Elsa Kania, Paul Triolo. *Full translation: China's New Generation Artificial Intelligence Development Plan (2017)*, Stanford University DigiChina Project, 1 August 2017, online.
136 State Council, 'Notice of the State Council on the publication of "Made in China 2025"', PRC Government, May 2015, online.
137 Wanyu Zhang, Ashwin Kaja, Yan Luo, Sean Stein, 'Spotlight Series on Global AI Policy—Part III: China's policy approach to artificial intelligence', *Inside Global Tech*, 8 February 2024, online.
138 David Lague, Paul Triolo. 'Three takeaways from China's new standards strategy', Carnegie Endowment for International Peace, 28 October 2021, online.
139 Yi Wu. 'China Standards 2035 Strategy: Recent developments and their implications for foreign companies', *China Briefing*, 26 July 2022, online.
140 'China's safety requirements for generative AI', translation, Georgetown Center for Security and Emerging Technology, 4 April 2024, online.
141 Amie Stepanovich, 'China's new AI governance initiatives shouldn't be ignored', Carnegie Endowment for International Peace, 4 January 2022, online.
142 'Xi Jinping attends video summit on Belt and Road digital economy development', Belt and Road Forum for International Cooperation, 2023, online.
143 State Council Information Office, 'SCIO press conference on China's policies and measures for opening-up', PRC Government, 17 November 2022, online.
144 'REAIM 2023: Call to action', Netherlands Government, 16 February 2023, online.
145 'European approach to artificial intelligence', European Commission, April 2024, online.
146 Carlos Ureña, *Regulating artificial intelligence: legal and ethical implications*, Oxford University Press; Anu Bradford, 'The European rights-driven regulatory model', in *Digital empires: the global battle to regulate technology*, Oxford Academic Books, September 2023, 105–146, online; 'Ethical and policy implications of artificial intelligence: towards a comprehensive approach', briefing, European Parliament Research Service, 2024, online.
147 Emily Rauhala, 'All about the EU's DSA and DMA laws to rein in big tech platforms', *Washington Post*, 6 September 2023, online.
148 'Shared vision, common action: a stronger Europe: a global strategy for the European Union's foreign and security policy', European Union, June 2016, online.
149 'Press release: The EU proposes a regulatory framework for AI', European Commission, online.
150 'Deputy Director-General—Chief Standardisation Officer', *EU Whoiswho*, European Union, 2024, online.
151 'EU AI Act: First regulation on artificial intelligence', European Parliament, 19 December 2023, online.
152 Charlotte Siegmann, Markus Anderljung, *The Brussels effect and artificial intelligence: how EU regulation will impact the global AI market*, Centre for the Governance of AI, August 2022, online.
153 Marianna Drake, Marty Hansen, Lisa Peets, 'EU and US lawmakers agree to draft AI code of conduct', *Inside Privacy*, 9 June 2023, online.
154 Sam Jungyun Choi, Dan Cooper, Diane Valat, 'EU digital partnerships with Asia: a new path towards enhanced digital collaboration and opportunities', *Global Policy Watch*, 12 January 2023, online.
155 'Maintaining American leadership in artificial intelligence', executive order, The White House, Washington DC, 14 February 2019, online; 'Safe, secure, and trustworthy development and use of artificial intelligence', executive order, The White House, Washington DC, 1 November 2023, online.
156 'Fact sheet: CHIPS and Science Act will lower costs, create jobs, strengthen supply chains, and counter China', The White House, Washington DC, 9 August 2022, online.
157 'Maintaining American leadership in artificial intelligence'; 'Safe, secure, and trustworthy development and use of artificial intelligence'.

158 Rachel Wright, *Artificial intelligence in the states: emerging legislation*, Council of State Governments, 6 December 2023, online.
159 'US Government National Standards Strategy for Critical and Emerging Technology 2023', The White House, Washington DC, May 2023, online.
160 'Maintaining American leadership in artificial intelligence'; Department of the Prime Minister and Cabinet, 'Quad Principles for Critical and Emerging Technology Standards', Australian Government, 20 May 2023, online.
161 'US leadership in AI: A plan for federal engagement in developing technical standards and related tools', NIST, August 2019, online.
162 NIST, 'American competitiveness of a More Productive Emerging Tech Economy Act', July 2023, online; 'Blueprint for an AI Bill of Rights', The White House, Washington DC, no date, online.
163 Department of Commerce, 'Department of Commerce to undertake key responsibilities in historic artificial intelligence executive order', US Government, 30 October 2023, online.
164 'Quad Leaders' Summit fact sheet', The White House, Washington DC, 20 May 2023, online.
165 Department of Commerce, 'Remarks by Commerce Secretary Gina Raimondo at the AI Safety Summit 2023 in Bletchley, England', US Government, 2 November 2023, online.
166 State Department, 'Political declaration on responsible military use of artificial intelligence and autonomy', US Government, 2023, online.
167 'AI risk management framework', NIST, April 2024, online.
168 Department of Industry, Science and Resources (DISR), 'Critical Technologies Statement', Australian Government, 22 May 2023, online.
169 DISR, 'Technology', Australian Government, no date, online.
170 Department of Home Affairs (DHA), *Australian Cyber Security Strategy 2023–2030*, Australian Government, 32, online.
171 'Ethical policy statement', New South Wales Government, 2022, online.
172 DHA, *Australian Cyber Security Strategy 2023–2030*.
173 DHA, *Australian Cyber Security Strategy 2023–2030*.
174 DISR, 'Critical Technologies Statement'.
175 DISR, *Safe and responsible AI in Australia consultation: Australian Government's interim response*, Australian Government, 2024, online.
176 DISR, 'The Bletchley declaration by countries attending the AI Safety Summit, 1–2 November 2023', Australian Government, 2 November 2023, online.
177 Department of the Prime Minister and Cabinet, 'Quad principles on critical and emerging technology standards', Australian Government, May 2023, online.
178 DISR, 'Australia and Singapore show compatibility between AI governance framework', Australian Government, 13 February 2024, online.
179 Bureau of Indian Standards, *Standards National Action Plan 2022–2027*, Indian Government, online.
180 'Quad Leaders' joint statement', The White House, Washington DC, May 2023, online.
181 Prime Minister's Office, 'PM inaugurates ITU area office and innovation centre', Indian Government, 22 March 2023, online.
182 Ashutosh Kumar, 'Early contribution to standardisation to help India lead 6G revolution: Reliance Jo, Bhart Airtel', ET Telecom, 18 March 2024, online.
183 'Quad principles on critical and emerging technology standards'.
184 Hideki Tomoshige, *The strategic convergence of the US–India innovation partnership*, Center for Strategic and International Studies, 22 December 2023, online.
185 'First EU–India trade and technology council focused on deepening strategic engagement on trade and technology', European Commission, 16 May 2023, online.
186 Cabinet Office of Japan, 'Society 5.0', Accessed April 2024, online.
187 Cabinet Office of Japan, 'AI Strategy 2020', April 2022, online.
188 Hiroki Habuka, 'Japan's approach to AI regulation and its impact on the 2023 G7 presidency'. Center for Strategic and International Studies, 14 February 2023, online
189 Aidan Arasasingham, Matthew Goodman, *Operationalizing data free flow with trust*, Center for Strategic and International Studies, 13 April 2023, online.
190 Government of Japan, 'Hiroshima AI Process G7 Digital & Tech Ministers' Statement', 1 December 2023, online.
191 'Smart Nation: the way forward: executive summary', Singapore Government, 2018, online.
192 'Smart Nation: the way forward: executive summary'.
193 Singapore Government, *Model Artificial Intelligence Governance Framework*, 2nd edition, 2020, online.
194 AI Verify foundation, online.
195 Singapore Government, 'Summary', *National Artificial Intelligence Strategy: Advancing our smart nation journey*, November 2019, online.
196 Singapore Government, *Singapore National AI Strategy 2.01: AI for the public good for Singapore and the world*, December 2023, online.
197 *Singapore National AI Strategy 2.01: AI for the public good for Singapore and the world*.

198 'US–Singapore Critical and Emerging Technology Dialogue: joint vision statement', The White House, Washington DC, 12 October 2023, online.
199 Elizabeth Law, 'From food security to therapeutic gardens: Singapore, China sign over 20 MoUs', *The Straits Times*, 8 December 2023, online.
200 Association of Southeast Asian Nations (ASEAN), *ASEAN Digital Masterplan 2025*, 2021, online.
201 Elina Noor, 'Southeast Asia's digital future should be more than replicas of the past', *South China Morning Post*, 1 March 2023, online.
202 ASEAN, 'ASEAN Telecommunications and Information Technology Ministers Meeting: Framework on digital data governance', December 2018, online.
203 ASEAN, 'ASEAN data management framework: data governance and protection throughout the data lifecycle', January 2021, online.
204 ASEAN, 'Digital Trade Standards and Conformance Working Group: work programme 2021–2025', online.
205 'About us', ASEAN–Australia Digital Trade Standards Initiative, no date, online.
206 ASEAN, *ASEAN guide on AI governance and ethics*, 2024, online.
207 Similar to the constellation of independent and autonomous Internet Governance Forums that take place nationally, regionally and at the global level but operate in the spirit of the same overarching principles, objectives and modalities. See: UN Internet Governance Forum, 'National and regional IGF initiatives', Accessed April 2024, online.
208 'Who is leading the critical technology race?', *Critical Technology Tracker*, ASPI, Canberra, 2024, online; Jamie Gaida, Jennifer Wong Leung, Stephan Robin, Danielle Cave, *ASPI's Critical Technology Tracker: sensors and biotech updates*, ASPI, Canberra, 22 September 2023, online.
209 IEEE Standards Association, 'IEEE introduces new program for free access to AI ethics and governance standards', 17 January 2023, online.
210 'Women in International Security and Cyberspace fellowship', Accessed April 2024, online.
211 'Let's talk cyber' was a series of informal multistakeholder dialogue in support of the government-to-government UN Working Group on ICT Security. *Let's Talk Cyber*, online.
212 ASPI's The Sydney Dialogue, online.
213 Kathy Nicholsen, Adam Slonim, *Artificial intelligence: your questions answered*, ASPI, Canberra, 11 April 2020, online; 'What is artificial intelligence (AI)?', IBM, 2024, online.
214 DISR, 'Technology'.
215 'Overview: Disruptive technology', *Oxford Reference*, online.
216 Ahmed Alsharif, 'Emerging technologies', in *Understanding technology*, Utah Valley University, online.
217 Brigitte Nerlich, 'Frontier AI: tracing the origin of a concept', University of Nottingham, online.
218 Elliot Jones, 'Explainer: What is a foundation model?', Ada Lovelace Institute, 17 July 2023, online.
219 'What is generative AI?', McKinsey & Company, no date, online; Sabrina Ortiz, 'What is generative AI and why is it so popular? Here's everything you need to know', *ZD Net*, 23 April 2024, online.
220 Akash Kesrwani, 'What are LLM (large language model)?', *Medium*, 4 July 2023, online.
221 'Organizations developing standards', Standards Coordinating Body, no date, online.

Acronyms and abbreviations

AI	artificial intelligence
ANSI	American National Standards Institute
ASEAN	Association of Southeast Asian Nations
ASPI	Australian Strategic Policy Institute
BIS	Bureau of Indian Standards
CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
CIS	Centre for Internet and Society
DFAT	Department of Foreign Affairs and Trade (Australia)
EU	European Union
GPAI	Global Partnership on AI
ICT	information and communications technology
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IP	internet protocol
ISBs	international standards bodies
ISO	International Organization for Standardization
IT	information technology
ITU	International Telecommunication Union
ITU-T	ITU Telecommunication Standardization Sector
JISC	Japanese Industrial Standards Committee
JTC1/SC42	Subcommittee 42 of the Joint Technical Committee 1 of the ISO and IEC
LLM	large language model
METI	Ministry of Economy, Trade and Industry (Japan)
ML	machine learning
NATO	North Atlantic Treaty Organization
NCs	national committees
NIST	National Institute of Standards and Technology (US)
NSBs	national standards bodies
OECD	Organisation for Economic Co-operation and Development
Quad	Quadrilateral Security Dialogue
R&D	research and development
RFC	request for comment
RSBs	regional standards bodies
SDOs	standards-developing organisations
SEP	standard essential patent
UN	United Nations
UNESCO	UN Educational, Scientific and Cultural Organisation
WTO	World Trade Organization


ASPI
AUSTRALIAN
STRATEGIC
POLICY
INSTITUTE


Centre
for Internet
& Society