

RCMUN 2026, AI Governance

Forum: AI Governance

Issue 2: The question of safeguarding intellectual property, strategic technologies, and sensitive data in the development of artificial intelligence systems, with particular focus on companies such as OpenAI, NVIDIA, Microsoft, Google DeepMind, TSMC, and ASML.

Student Officer: Juan Maldonado

Safeguarding intellectual property, strategic technologies and sensitive data in the development of artificial intelligence systems

Articles:

<https://www.morganlewis.com/pubs/2026/01/bis-revises-export-review-policy-for-advanced-ai-chips-destined-for-china-and-macau>

https://www.banking.senate.gov/imo/media/doc/letter_to_commerce_nvidia_supermicro.pdf

https://www.rand.org/pubs/research_reports/RRA2849-1.html

<https://arxiv.org/pdf/2602.21012>

<https://www.un.org/global-dialogue-ai-governance/en>

<https://news.un.org/en/story/2026/07/1167862>

<https://www.unesco.org/en/articles/global-dialogue-ai-governance-geneva-6-7-july>

<https://eto.tech/blog/five-key-facts-chokepoints-chip-supply-chain/>

<https://www.gibsondunn.com/eu-ai-act-omnibus-agreement-postponed-high-risk-deadlines-and-other-key-changes/>

<https://www.taiwannews.com.tw/news/6348529>

<https://thediplomat.com/2026/07/singaporean-police-seize-42m-bungalow-in-nvidia-chip-smuggling-probe/>

<https://www.ohchr.org/en/meeting-summaries/2026/07/human-rights-council-concludes-sixty-second-regular-session-after>

Videos:

<https://webtv.un.org/en/asset/k1v/k1vqmc2dm7>

<https://webtv.un.org/en/asset/k1y/k1yd3dlebq>

<https://www.itu.int/en/mediacentre/Pages/MA-2026-06-02-UN-Dialogue.aspx>

Key Terms:

- **Intellectual property (IP):** the body of rights protecting creations of the mind. Three branches matter here: patents, which protect disclosed inventions for a limited period; copyright, which protects original expression and is at the centre of the training-data disputes; and trade secrets, which protect commercially valuable information precisely because it is not disclosed.
- **Trade secret:** confidential business information that derives its value from secrecy and is subject to reasonable steps to keep it secret. Protected internationally under Article 39 of the TRIPS Agreement as 'undisclosed information'. Unlike a patent, a trade secret is never published, which is why it is the preferred protection for chip processes, model architectures and training recipes.

- **Model weights:** the numerical parameters produced by training an AI model. They are the model: whoever holds the weights holds a working copy of a system that may have cost hundreds of millions of dollars in compute to create. Weights are treated by developers as their single most sensitive asset, and by security researchers as a plausible target for state-level espionage.
- **Frontier model / general-purpose AI (GPAI):** a model at or near the most capable systems of its time, trainable for a wide range of tasks. The EU AI Act uses the term general-purpose AI model and imposes documentation, copyright-policy and systemic-risk obligations on its providers.
- **Distillation:** training a smaller model on the outputs of a larger one, so that the second model reproduces much of the first model's capability without access to its weights. Because it requires only query access, distillation is a route to appropriating the value of a model without ever breaching its security perimeter.
- **Compute:** the processing capacity used to train and run AI systems, measured in operations per second. Compute is currently the most governable input to AI, because it is physical, concentrated, and produced by a small number of firms.
- **Total Processing Performance (TPP):** the performance metric the United States uses to define which chips are controlled. Chips above the threshold require an export licence; the metric is set out in Export Control Classification Number 3A090 and has been revised repeatedly since October 2022.
- **Export controls:** national restrictions on the transfer of goods, software and technology across borders on security grounds. Dual-use controls cover items with both civilian and military applications, which is how advanced chips and chipmaking tools are classified.
- **Foreign Direct Product Rule (FDPR):** a United States rule extending its jurisdiction to goods made anywhere in the world using American technology or software. It is the principal mechanism by which US controls reach non-US companies, and the principal reason other states describe those controls as extraterritorial.
- **Transshipment and diversion:** the routing of controlled goods through a third country to disguise their true destination. Enforcement cases since 2025 have centred on Singapore, Malaysia and Taiwan, and have largely been brought as fraud rather than as export-control offences.
- **Chokepoint:** a stage of production controlled by so few suppliers that access can be denied. The clearest example is extreme ultraviolet (EUV) lithography, made only by ASML in the Netherlands, using optics made only by Carl Zeiss SMT in Germany.
- **Text and data mining (TDM) exception:** a provision in copyright law permitting the automated analysis of lawfully accessed works. The EU exception under the 2019 Copyright Directive, with its opt-out for rightsholders, is the framework against which most European AI training disputes are argued.
- **Data provenance:** documented evidence of where training data came from, under what licence, and with what consent. Provenance is the practical precondition for almost every remedy discussed in this committee, and it is the thing that is most often missing.
- **Know-your-customer (KYC) and end-use verification:** due diligence obligations requiring an exporter to establish who the ultimate user of a controlled item is and what they will do with it. The January 2026 US rule makes such certifications a condition of licensing.

- **Hardware-enabled governance:** proposals to build verification directly into chips, for example on-chip location attestation, so that compliance can be confirmed without physical inspection. Supporters see it as the only scalable enforcement tool; critics see a surveillance capability embedded in general-purpose hardware.
- **Compute divide:** the gap between the small number of states and firms with access to frontier training capacity and everyone else. The Global Digital Compact identifies closing this gap as a development objective; export controls, by design, widen it for some states.
- **UN Guiding Principles on Business and Human Rights (UNGPs):** the authoritative global standard, endorsed by the Human Rights Council in 2011, setting out the state duty to protect, the corporate responsibility to respect, and access to remedy. They are the Council's existing route to addressing conduct by private AI developers.
- **Right to science (ICESCR Article 15):** the right of everyone to enjoy the benefits of scientific progress and its applications, held in the same article as the right of authors to protection of their material and moral interests. The tension between those two limbs is, in miniature, the tension before this committee.

Overview:

Artificial intelligence is built from three inputs that are easy to steal and hard to govern: intellectual property, in the form of model architectures and manufacturing processes; strategic technologies, above all semiconductors and the machines that make them; and data, both copyrighted works and the personal information swept up alongside them. Trade secrecy protects by concealment, copyright by permission, export control by prohibition, data protection by consent. None of these regimes was designed for the others.

That absence of coordination is this committee's subject. The Global Digital Compact of September 2024 committed states to interoperable rather than fragmented governance, and in August 2025 the General Assembly created the Independent International Scientific Panel on AI and the Global Dialogue on AI Governance, which first met in Geneva in July 2026. UNESCO's 2021 Recommendation and the OECD AI Principles supply normative content; no forum yet supplies a settlement between the security, commercial and rights claims made over AI's inputs.

The defining fact is concentration. ASML alone makes EUV lithography systems, TSMC fabricates most of the world's advanced logic chips, a few American firms supply almost all chip design software, and NVIDIA designs the accelerators behind most frontier training. Who may use advanced AI is decided, in practice, by a handful of companies and governments.

Those decisions are made through export control. The United States has restricted advanced chips since October 2022, easing to case-by-case review for China in January 2026 while extending licence requirements worldwide in May. China has answered through its dominance of critical minerals. Enforcement has followed: Singapore is prosecuting the largest known diversion case as fraud, and in April 2026 a Taiwanese court jailed a former TSMC engineer for ten years over 2-nanometre secrets.

On data, courts have moved fastest in the absence of legislation (the USD 1.5 billion Anthropic settlement, *Getty v. Stability AI*, the unresolved New York Times case) while the EU deferred its high-risk AI rules to 2027.

RCMUN 2026, AI Governance

The difficulty is structural. These firms are governed only indirectly, through the states that host them; the UN's new machinery can convene but cannot compel; and the states most exposed to the fragmentation had least say in writing the rules.

Statistics and Infographics:

Safeguarding IP, strategic technologies and data in AI

Key events, 2018–2026

CONTROLS BEGIN - 2018-2022

- Aug 2018 • US Export Control Reform Act creates 'emerging and foundational technology' category
- 2019 • Netherlands withholds ASML EUV export licence for China
- Oct 2022 • BIS introduces performance thresholds (TPP) on advanced computing chips

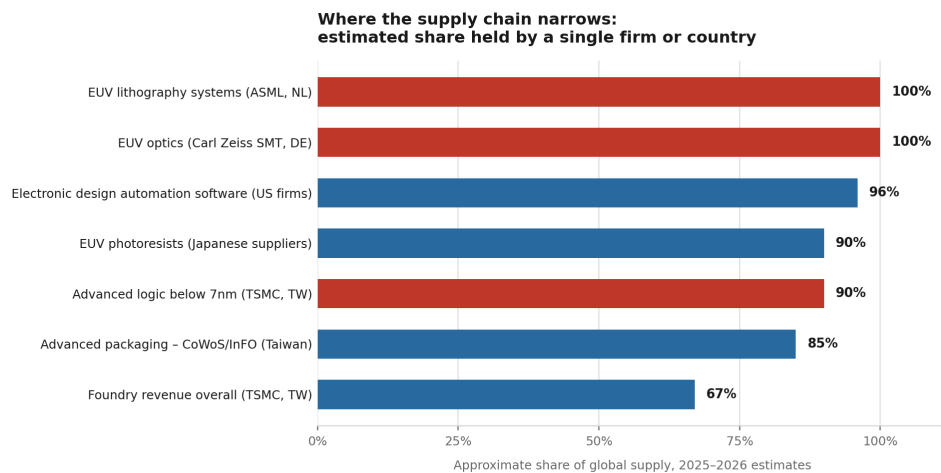
EXPANSION - 2023-2025

- Oct 2023 • Thresholds revised; end-use and country scope widened
- Dec 2023 • New York Times sues OpenAI and Microsoft over training data
- Sep 2024 • UN Global Digital Compact adopted at the Summit of the Future
- Dec 2024 • China bans exports of gallium, germanium and antimony to the US
- Apr 2025 • China restricts seven medium and heavy rare earth elements
- Aug 2025 • EU AI Act obligations for general-purpose AI models take effect
- Sep 2025 • Bartz v. Anthropic settles for US\$1.5bn, largest US copyright settlement
- Nov 2025 • UK High Court rules in Getty Images v. Stability AI
- Dec 2025 • Reuters reports a prototype EUV machine assembled in Shenzhen

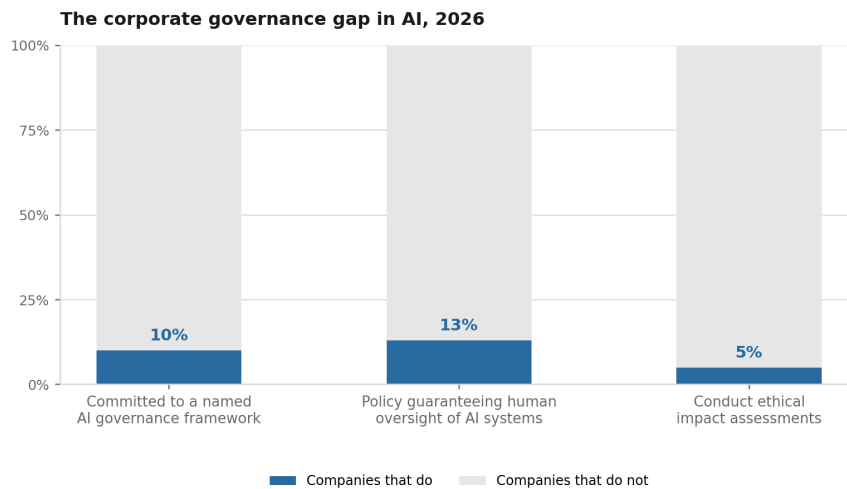
CONVERGENCE - 2026

- Jan 2026 • BIS moves H200-class exports to China from denial to case-by-case review
- Mar 2026 • US indicts three, incl. a Supermicro co-founder, over ~\$510m in diverted servers
- Apr 2026 • Taiwan jails ex-TSMC engineer for 10 years over 2nm process secrets
- Apr 2026 • MATCH Act clears House Foreign Affairs Committee
- May 2026 • BIS guidance extends licence requirements to D:5-headquartered firms worldwide
- Jun 2026 • US-ASML dispute over alleged EUV-related shipments becomes public
- Jul 2026 • First UN Global Dialogue on AI Governance convenes in Geneva
- Jul 2026 • EU Digital Omnibus defers AI Act high-risk obligations to December 2027

Sources: US Bureau of Industry and Security; European Commission; Reuters; Taiwan Intellectual Property and Commercial Court; United Nations



Sources: Emerging Technology Observatory (CSET); industry supply-chain analyses. Figures are widely cited estimates, not official statistics.



Source: The AI Company Data Initiative, Thomson Reuters Foundation with UNESCO, March 2026.

Major Parties:

The United States: the state that sets the terms of the current regime. It hosts the leading model developers, the dominant chip designer and almost the entire electronic design automation industry, and it has used export controls, the Foreign Direct Product Rule and criminal enforcement as its principal instruments. Its position is that restrictions on advanced compute are a national security necessity; its critics, including several allies, object less to the objective than to the unilateral and extraterritorial method.

China: the principal target of the controls and the principal source of counter-pressure. Beijing frames the restrictions as containment dressed as security, points to their effect on global supply chains, and has responded through its dominance of critical minerals processing while accelerating domestic substitution in lithography, chipmaking and open-weight model development. It is also the state most frequently identified in Western enforcement actions concerning diverted hardware and appropriated technical information.

The Netherlands and the European Union: the Netherlands hosts ASML and therefore holds the single most consequential chokepoint in the chain, a position it did not seek and cannot easily hedge. The European Union has taken the opposite regulatory approach to the United States, legislating comprehensively through the AI Act while deferring its most demanding obligations, and it leads on data protection and on transparency duties for general-purpose models. The EU also spoke at the first Global Dialogue in favour of a credible independent scientific baseline for AI governance.

Taiwan: manufactures the great majority of the world's most advanced logic chips and now treats its process technology as national core key technology, prosecuting leaks under national security law rather than commercial law. Taiwan's exposure is doubled: it is both the indispensable supplier and the geopolitical fault line, and its enforcement decisions set the practical standard for how the industry protects technical information.

Japan and the Republic of Korea: suppliers of the materials, equipment and memory without which nothing else functions, from photoresists and mask blanks to high-bandwidth memory. Both have

aligned with United States controls to varying degrees while resisting formal obligations to do so, and Japanese firms have been implicated in the Taiwanese trade secret litigation.

Singapore, Malaysia and the United Arab Emirates: third countries through which controlled hardware has been routed, and which are now developing enforcement doctrines of their own. Singapore's use of ordinary fraud and money laundering law rather than export control law is the most significant procedural development in this area, and one other states may replicate. These states also illustrate the burden that unilateral controls place on jurisdictions that did not adopt them.

Frontier model developers (OpenAI, Google DeepMind, Anthropic, Microsoft, Meta): hold the weights, the training data and the algorithmic secrets at issue, and are simultaneously the claimants in some disputes and the defendants in others. Their security practices vary considerably and are largely unverified by any external body. They are not bound by human rights treaties but are covered by the corporate responsibility to respect under the Guiding Principles, and their disclosure choices determine what any regulator can actually see.

NVIDIA, TSMC and ASML: the three firms whose products define the physical chokepoints. Each has argued publicly that export restrictions imposed on it either fail to achieve their objective or transfer the market to competitors, and each has been the subject of official scrutiny over compliance during 2026. Their commercial interests and their governments' security interests are not identical, which is itself a governance problem.

Rightsholders, authors and the creative sector: publishers, image libraries, authors' associations, musicians and journalists whose works were used in training without licence. Their claims rest on Article 15 of the ICESCR as much as on domestic copyright, and their remedies to date have come from litigation and private settlement rather than from any public framework. Collective licensing bodies and press publishers are pressing for statutory solutions in several jurisdictions.

OHCHR and the Council's own mechanisms: the B-Tech Project provides the authoritative guidance on applying the Guiding Principles in the technology sector; the Working Group on Business and Human Rights reported to the Council on AI procurement and deployment in 2025; the Special Rapporteurs on privacy, on freedom of expression and on cultural rights each hold relevant mandates; and the Advisory Committee is preparing a study on the impact of AI systems on good governance under resolution 57/5.

UNESCO, WIPO and the WTO: UNESCO's 2021 Recommendation on the Ethics of Artificial Intelligence remains the only near-universal normative instrument in the field and is implemented through its Readiness Assessment Methodology. WIPO convenes the standing conversation on AI and intellectual property. The WTO administers TRIPS, including the Article 39 protection of undisclosed information, and the security exception in Article XXI GATT is the provision on which export controls ultimately rest.

The Global Dialogue on AI Governance and the Independent International Scientific Panel: established by the General Assembly in August 2025 and convened for the first time in Geneva in July 2026, co-chaired by El Salvador and Estonia and, for the Panel, by Yoshua Bengio and Maria Ressa.

States without frontier capacity: the substantial majority of this Council. They are neither the source of the technology nor the target of the controls, but they inherit the consequences: dependence on

systems they cannot audit, exposure to supply chains they cannot influence, and rules on access to compute written without them.

Possible Solutions:

Artificial intelligence is built from three inputs that are easy to steal and hard to govern: intellectual property, in the form of model architectures and manufacturing processes; strategic technologies, above all semiconductors and the machines that make them; and data, both copyrighted works and the personal information swept up alongside them. Trade secrecy protects by concealment, copyright by permission, export control by prohibition, data protection by consent. None of these regimes was designed for the others.

This is a human rights question. Article 15 of the ICESCR protects both the right to share in the benefits of science and the rights of authors, and the training-data disputes are a collision between the two. Article 17 is engaged whenever personal data is scraped without a lawful basis, Article 19 whenever trade secrecy shields consequential systems from scrutiny. The UN Guiding Principles already frame the conduct of the firms named here.

The defining fact is concentration. ASML alone makes EUV lithography systems, TSMC fabricates most advanced logic chips, and NVIDIA designs the accelerators behind most frontier training. Who may use advanced AI is decided by a handful of companies and governments.

Those decisions are made through export control. The United States has restricted advanced chips since October 2022, easing to case-by-case review for China in January 2026 while extending licence requirements worldwide in May. China has answered through critical minerals. Enforcement has followed: Singapore is prosecuting the largest known diversion case as fraud, and in April 2026 a Taiwanese court jailed a former TSMC engineer for ten years over 2-nanometre secrets.

On data, courts have moved fastest — the USD 1.5 billion Anthropic settlement, *Getty v. Stability AI*, the unresolved New York Times case — while the EU deferred its high-risk AI rules to 2027.

The difficulty is structural. These firms are not parties to human rights treaties, the UN's new AI machinery can compel nothing, and the states most affected had least say in writing the rules.

Committee Objective:

The goal of the AI Governance Council at RCMUN is to establish how the protection of intellectual property, strategic technologies and sensitive data in artificial intelligence can be reconciled with the rights of the people affected by those systems. Delegates are asked to treat this not as a contest between innovation and regulation, but as a question about who decides: who may access the technology, who may inspect it, who is compensated when their work or their data is used to build it, and who is left dependent on systems they had no part in shaping.

By examining the positions of the major parties and the wider implications for the international human rights system, the committee should reach a resolution that recognises legitimate security and commercial interests while insisting that measures taken to defend them meet the tests of legality,

necessity and proportionality. Keeping in mind the legal, economic and technological dimensions of the problem, delegates should strive for rigorous debate directed towards collective action rather than declaratory consensus.

In order to fulfil these goals, nations should work towards resolutions addressing such matters as: transparency and provenance obligations for training data; confidential audit mechanisms that survive trade secret protection; rights-based conditions on export control, verification and hardware attestation regimes; remuneration and remedy for authors and data subjects; human rights due diligence across the full AI value chain, including its upstream labour and mineral components; and equitable access to compute and to the benefits of scientific progress, so that the outcome protects the assets of the developed AI economy without ratifying the exclusion of everyone else from it.

Sources:

- Baker McKenzie. "BIS Revises License Review Policy for Advanced Computing Commodities (AI Semiconductors) to China and Macau." Global Sanctions and Export Controls Blog, 28 January 2026, sanctionsnews.bakermckenzie.com.
- Bengio, Yoshua, et al. International AI Safety Report 2026. 2026, arxiv.org/pdf/2602.21012.
- Bureau of Industry and Security. "Revision to License Review Policy for Advanced Computing Items." Federal Register, doc. 2026-00789, effective 15 January 2026.
- Congressional Research Service. U.S. Export Controls and China: Advanced Semiconductors. CRS, June 2026, www.congress.gov.
- Diplomat, The. "Singaporean Police Seize \$42M Bungalow in Nvidia Chip Smuggling Probe." The Diplomat, 2 July 2026, thediplomat.com/2026/07/singaporean-police-seize-42m-bungalow-in-nvidia-chip-smuggling-probe/.
- Emerging Technology Observatory. "Beyond TSMC and EUV: Five Key Points on Chip Chokepoints." Center for Security and Emerging Technology, eto.tech/blog/five-key-facts-chokepoints-chip-supply-chain/.
- European External Action Service. "Global Dialogue on Artificial Intelligence Governance: EU Statement." EEAS, 7 July 2026, www.eeas.europa.eu.
- Gibson Dunn. "EU AI Act Omnibus Agreement: Postponed High-Risk Deadlines and Other Key Changes." Gibson Dunn, 27 May 2026, www.gibsondunn.com.
- International Telecommunication Union. "Global Dialogue on AI Governance, Geneva, 6-7 July." ITU, 2 June 2026, www.itu.int/en/mediacentre/Pages/MA-2026-06-02-UN-Dialogue.aspx.
- Mayer Brown. "Administration Policies on Advanced AI Chips Codified, with Reverberations Across AI Ecosystem." Mayer Brown, 22 January 2026, www.mayerbrown.com.
- Miller, Chris. Chip War: The Fight for the World's Most Critical Technology. Scribner, 2022.
- Nevo, Sella, et al. Securing AI Model Weights: Preventing Theft and Misuse of Frontier Models. RAND Corporation, RR-A2849-1, 2024, www.rand.org/pubs/research_reports/RAA2849-1.html.

Office of the High Commissioner for Human Rights. B-Tech Project: Applying the UN Guiding Principles on Business and Human Rights to Digital Technologies. OHCHR, www.ohchr.org/en/business-and-human-rights/b-tech-project.

Office of the High Commissioner for Human Rights. "Human Rights Council Advisory Committee Concludes Its 34th Session." OHCHR, 20 February 2026, www.ohchr.org.

Office of the High Commissioner for Human Rights. "Human Rights Council Concludes Sixty-Second Regular Session after Adopting 28 Resolutions." OHCHR, 8 July 2026, www.ohchr.org.

Organisation for Economic Co-operation and Development. Due Diligence Guidance for Responsible AI. OECD, 2026.

Taiwan News. "Former TSMC Engineer Sentenced to 10 Years for Leaking 2nm Trade Secrets." Taiwan News, 27 April 2026, www.taiwannews.com.tw/news/6348529.

Thomson Reuters Foundation and UNESCO. The AI Company Data Initiative. March 2026.

UNESCO. Recommendation on the Ethics of Artificial Intelligence. UNESCO, 2021, www.unesco.org.

UNESCO. "Global Dialogue on AI Governance, Geneva, 6-7 July." UNESCO, July 2026, www.unesco.org/en/articles/global-dialogue-ai-governance-geneva-6-7-july.

United Nations. Global Digital Compact. Summit of the Future, September 2024, www.un.org/global-digital-compact.

United Nations General Assembly. Terms of Reference and Modalities for the Independent International Scientific Panel on Artificial Intelligence and the Global Dialogue on Artificial Intelligence Governance. Adopted August 2025, www.un.org/global-dialogue-ai-governance/en.

United Nations Human Rights Council. Report of the Working Group on Business and Human Rights: Artificial Intelligence Procurement and Deployment. A/HRC/59/53, 2025.

UN News. "Global Push for AI Governance amid Warnings of 'Catastrophic Harm'." UN News, 5 July 2026, news.un.org/en/story/2026/07/1167862.

United States Senate Committee on Banking, Housing, and Urban Affairs. Letter to Secretary of Commerce Howard Lutnick on the Diversion of Advanced AI Chips. 23 March 2026, www.banking.senate.gov.

World Trade Organization. Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), Article 39. WTO, www.wto.org/english/tratop_e/trips_e/trips_e.htm.