The Geopolitics of AI in Middle Powers

Project Summaries

Foreign Capital in the AI Supply Chain

Adam Hassan and Haley Yi | Supervised by Aris Richardson

Executive Summary

This memo maps foreign sovereign and institutional investment in frontier AI companies and sets out what the pattern means for AI safety funders pursuing middle power strategy, including Astralis, and for European policymakers weighing engagement with frontier AI. Two findings and three recommendations follow.

European institutional capital is largely absent from frontier AI, and only part of that absence is explainable. No European sovereign wealth fund or pension fund holds an equity position in OpenAI, Anthropic, or xAI. For European Union budgetary capital, the absence has a concrete explanation in the seven-year structure of the Multiannual Financial Framework, which locked in priorities before AI safety was a recognised one. For member state sovereign and pension funds, the absence is not yet explained, and that question is the more consequential one for funders to pursue.

Foreign capital has entered Chinese frontier AI in a low-leverage form. Arabian Gulf capital is present in Chinese frontier labs, but it enters as minority pre-IPO equity or as arms-length public-market participation, not as governance-proximate investment. The separation between the US frontier AI sector and the Chinese frontier AI sector is likely the outcome of US conditionality pressure rather than a fixed feature of the landscape.

For funders and policymakers, the memo identifies three areas for near-term work. These are understanding why European institutional capital has not engaged frontier AI, mapping the conditions under which investment proximity converts into governance influence, and modelling the contest that is shaping the US and China investor divide. Conditionality is the mechanism that links investment to influence, and while Europe is building procurement-based conditionality tools, it has not extended them to AI.

Purpose and Audience

This memo presents preliminary findings from an ongoing project mapping foreign sovereign and institutional investment in frontier AI companies. The intended outcome is to inform two sets of decisions.

The first set belongs to AI safety funders and foundations engaged in middle power strategy, including Astralis, which supports grant-making focused on middle power actors and their role in shaping global AI governance. The findings bear directly on how such a funder allocates research and convening budgets. The first finding implies a choice between commissioning research into why European institutional investors have not engaged frontier AI and supporting dialogue between those investors and AI safety researchers. The second finding implies a choice about whether to fund work that models the US and China investment divide as a contested and movable outcome rather than a settled one.

The second set of decisions belongs to European policymakers and institutional investors. The relevant decisions include whether and how to treat frontier AI as a fundable priority in the next European Union budget cycle, whether to attach conditionality to AI investment and procurement, and whether to encourage sovereign and pension engagement with the sector. A central finding of this memo is that European capital has not been activated toward frontier AI equity despite the scale of available assets, and that part of the explanation now has a clear institutional and calendar anchor.

The scale of the capital pools involved frames what is at stake. Sovereign wealth funds alone manage approximately $15.8 trillion globally as of March 2026, with funds based in the Middle East and North Africa accounting for 39% of that total and European funds for 17%.[1] When public pension funds and central bank reserves are included, total state-owned investor assets reach roughly $60.7 trillion, with Europe's share rising to about $11.5 trillion across all three vehicle types. European state-owned capital is therefore substantially larger than the Arabian Gulf states' in aggregate, which makes its absence from frontier AI equity a question worth explaining rather than assuming.

[1] Global SWF, sovereign wealth and state-owned investor asset data — https://globalswf.com/

The project's two original contributions are the documented absence of European sovereign and pension capital from frontier AI equity, and an account of the US and China investment divide as a contested outcome shaped by policy rather than a structural feature.

Methods and Scope

Research proceeded in two phases. The first phase built a structured tracker of confirmed deals and reported discussions between foreign sovereign investors and frontier AI companies, drawing on press reporting, official funding announcements, IPO prospectuses, and regulatory filings, with searches run systematically across Google News, Crunchbase, Tracxn, and regional business press including Arabian Business and Zawya. The second phase extended coverage to Chinese AI labs, adding Hong Kong Stock Exchange filings, where IPO prospectuses provide the most reliable pre-IPO shareholder data available. Large language models assisted with the classification and extraction of investor names, round details, and deal terms, and with cross-referencing entries for consistency. All extracted data was verified manually against primary sources before inclusion, and entries without a verifiable primary source were flagged as unconfirmed or excluded.

Inclusion followed two criteria. For companies, the tracker covers independent frontier AI labs with external funding rounds and documented investor disclosures, and excludes corporate AI divisions without independent funding rounds as well as founder-funded companies with no external investors, since the project's leverage question requires an identifiable investor relationship to analyse. For investors, the tracker captures sovereign wealth funds, national investment companies, and other state-linked vehicles as primary actors, alongside private and institutional co-investors that appear in the same rounds.

On the US side, the tracker covers OpenAI, Anthropic, and xAI. Google DeepMind and Meta AI are excluded as wholly owned corporate subsidiaries with no independent external funding rounds. On the China side, the tracker covers Zhipu AI, MiniMax, Moonshot AI, and 01.AI. DeepSeek is excluded as entirely founder-funded with no external investors to track. Manus is excluded following its acquisition by Meta in December 2025, after which Meta confirmed no continuing Chinese ownership. Corporate AI divisions inside Baidu, ByteDance, and Alibaba are

excluded on the same basis as DeepMind and Meta. Mistral AI is included as a reference case for the analysis of unactivated European capital.

Two limitations bear on how the findings should be read. The dataset is built primarily from English-language sources, and Chinese and Arabic-language regional coverage likely contains deal activity not indexed here. Individual investor contributions are rarely disclosed, and most financial figures reflect round sizes rather than specific allocations. The findings in this memo are based on Hong Kong prospectuses and filing-based reporting on a four-lab sample. Foreign participation in this sample arose mostly in 2024 and during the December 2025 to January 2026 listing wave. The project can document the presence of foreign capital but cannot establish its absence, so claims about Chinese labs in this memo are scoped to the four-lab sample rather than to Chinese frontier AI as a whole. The comparison of sovereign and pension funds that have not invested in frontier AI is being developed separately and will strengthen the regional comparison in future iterations.

Key Findings

Finding 1. European capital is largely absent from frontier AI, and only part of that absence is explainable

Across OpenAI, Anthropic, and xAI, no European sovereign wealth fund or pension fund holds an equity position. The non-US, non-Arabian Gulf equity picture is almost entirely Singaporean and Japanese capital. Singapore's GIC leads Anthropic's $30 billion Series G, Temasek holds positions in both Anthropic and the AI Infrastructure Partnership, and SoftBank has committed more than $40 billion to OpenAI across four rounds. Beyond those three actors, non-US non-Arabian Gulf equity participation across the three labs consists of the Ontario Teachers' Pension Plan in Anthropic's $13 billion Series F and Baillie Gifford in Anthropic's Series G.

European sovereign and pension funds do not appear in any equity position in any of the three labs. Their only presence in the capital structures of OpenAI and Anthropic is through bank debt, by way of institutions including UBS, Santander, HSBC, Barclays, and Royal Bank of Canada participating in revolving credit facilities arranged for OpenAI in October 2024 and Anthropic in May 2025. Debt carries no ownership stake and no governance rights.

This absence is not a question of insufficient capital. Norway's Government Pension Fund Global manages approximately $1.8 trillion, and the major European and Canadian pension funds, including APG, PGGM, CDPQ, and CPP Investments, represent several trillion more. Nor does the absence reflect a blanket aversion to AI investment. Mistral AI, a French frontier lab, has raised approximately $3 billion across five rounds since June 2023, drawing on European private and corporate capital throughout. European institutional capital has had opportunities to engage with frontier AI, domestically and internationally, but has mostly avoided them.

The reason for the absence appears to differ by vehicle, and separating the vehicles clarifies what kind of engagement is appropriate. For European Union budgetary capital, the explanation is partly visible and is structural. The Union's central budget is set through the Multiannual Financial Framework, a seven-year cycle, and under the current 2021 to 2027 framework roughly two-thirds of commitments are pre-allocated to agriculture and cohesion funding.[2][3] AI safety was not a recognised priority when the current cycle was programmed, so it was not budgeted, and the rigidity of the seven-year structure has limited the scope to redirect funds since. This is a recurring constraint rather than a permanent one. The Commission proposed the next framework, covering 2028 to 2034, in July 2025 at close to €2 trillion, with greater flexibility as an explicit design feature and with the research and innovation programme, Horizon Europe, proposed to nearly double to €175 billion.[4] Negotiations are expected to conclude in time for legal acts to be adopted during 2027.[5] The drafting of that framework is therefore a concrete and dated decision point at which AI safety could be programmed as a fundable priority.

---

[2] The 2028-2034 EU budget for a stronger Europe — https://commission.europa.eu/strategy-and-policy/eu-budget/long-term-eu-budget/eu-budget-2028-2034_en

[3] The MFF Package: An Ambitious Proposal from a Fragile Commission — https://institutdelors.eu/en/publications/the-mff-package-a-ambitious-proposal-from-a-fragile-commission/

[4] Horizon Europe 2028-2034: twice bigger, simpler, faster and more impactful — https://research-and-innovation.ec.europa.eu/news/all-research-and-innovation-news/horizon-europe-2028-2034-twice-bigger-simpler-faster-and-more-impactful-2025-07-16_en

[5] European Council meeting, 18 December 2025 — https://www.consilium.europa.eu/en/meetings/european-council/2025/12/18/

For member state sovereign wealth funds and pension funds, no equivalent explanation is yet available. The barrier may be regulatory constraints on private market exposure, political choice, or simple inattention, and the project has not determined which. That distinction matters, because each points to a different intervention, and resolving it is the more consequential of the two open questions in this finding. European institutions operate within democratic accountability structures and have demonstrated responsiveness to governance arguments in other asset classes. Their absence from frontier AI equity means they hold no seat at the investor level when these companies make decisions about safety, deployment, and the conditions they are willing to accept from investors.

Finding 2. Foreign capital has entered Chinese frontier AI in a low-leverage form, and the US and China investment divide is contested rather than structural

Of the four Chinese labs in the sample, three show documented foreign participation. Saudi Arabia's Prosperity7 Ventures, the venture arm of Saudi Aramco, holds a pre-IPO stake in Zhipu AI. The Abu Dhabi Investment Authority and the Korean firm Mirae Asset Securities invested in MiniMax at its January 2026 listing. An unnamed consortium of Southeast Asian investors participated in 01.AI's August 2024 round. Only Moonshot AI shows no foreign participation on current evidence.

Foreign entry into Chinese frontier AI is recent and accelerating. Prosperity7's participation in a Zhipu funding round in mid-2024, at a valuation of approximately $3 billion, was reported at the time as the first known foreign backing of a major Chinese generative AI company, which suggests that the investors' landscape was mostly domestic before 2024.[6] The December 2025 to January 2026 wave of Hong Kong listings, which followed a broad shift in global investor attention toward Chinese AI, then brought further foreign participation.[7]

---

[6] "Saudi Fund Joins $400 Million Financing for China AI Firm Zhipu," Bloomberg, May 2024 — https://www.bloomberg.com/news/articles/2024-05-31/saudi-fund-joins-400-million-financing-for-china-ai-firm-zhipu

[7] "AI IPOs Drive a Strong Start to 2026," HKEX Insight, 3 February 2026 — https://www.hkexgroup.com/Media-Centre/Insight/Insight/2026/Johnson-Chui/AI-IPOs-Drive-a-Strong-Start-to-2026?sc_lang=en

The form that foreign capital takes differs between the American and Chinese ecosystems. The US frontier labs remain private, so foreign capital there takes the form of pre-IPO equity, where a sovereign fund leading or co-leading a funding round sits close to the company. The Chinese frontier labs have largely moved to public markets, so foreign capital there arrives mostly as participation in the public listing. Zhipu is the pre-IPO case. Prosperity7 joined a private round as a minority investor and was the first foreign firm reported to back a major Chinese generative AI company on Zhipu's pre-IPO shareholder register.[8] MiniMax is the public-market case. The Abu Dhabi Investment Authority entered as a cornerstone investor at the IPO, committing approximately $65 million for 3.35 million shares, within a cornerstone tranche of roughly $350 million, and Mirae Asset Securities joined on the same basis.[9][10] A cornerstone investor commits before the listing to buy a fixed allocation at the offer price, is named in the prospectus, and accepts a lock-up period, but does not receive board representation or information rights.[11] Cornerstone participation therefore sits well below pre-IPO lead investment on any measure of governance proximity.

Foreign capital is a minority layer in both companies. Domestic and state-linked capital dominates the pre-IPO registers, including Alibaba, Ant Group, Tencent, Meituan, Xiaomi, and HongShan in the case of Zhipu. MiniMax listed through a weighted voting rights structure that leaves its founders in voting control, so the equity that any outside investor holds is non-controlling by design. The implication for the project's leverage question is that foreign and Arabian Gulf leverage over Chinese frontier labs through equity is minimal. This is not because

---

[8] Knowledge Atlas Technology Joint Stock Company Limited (Zhipu AI), Global Offering prospectus dated 30 December 2025, HKEX — https://www1.hkexnews.hk/listedco/listconews/sehk/2025/1230/2025123000017.pdf

[9] "China's AI startup MiniMax Group raises $619 million in Hong Kong IPO," Reuters, 8 January 2026 — https://www.reuters.com/world/asia-pacific/chinas-ai-startup-minimax-group-raises-619-million-hong-kong-ipo-2026-01-08/ ; cornerstone allocation detail, AGBI, December 2025 — https://www.agbi.com/finance/2025/12/adia-backs-ipo-of-chinese-ai-startup-minimax/

[10] Adia backs IPO of Chinese AI startup MiniMax — AGBI, 31 December 2025 — https://www.agbi.com/finance/2025/12/adia-backs-ipo-of-chinese-ai-startup-minimax/

[11] MiniMax Group Inc., Global Offering prospectus dated 31 December 2025, HKEX — https://www1.hkexnews.hk/listedco/listconews/sehk/2025/1231/2025123100025.pdf

foreign exposure is absent, but because the exposure that exists arrives in a form that does not convert into governance influence. Even Zhipu, the higher-proximity case, involved a minority stake rather than a lead position.

The separation between the US and Chinese investor bases is therefore better understood as a contested outcome than as a structural fact. Arabian Gulf capital has a commercial interest in exposure to both ecosystems and has acted on that interest. The countervailing force is US conditionality. The clearest instance is the requirement that G42 divest its Chinese technology holdings as a condition of Microsoft's investment, and reporting on the Zhipu round noted that it coincided with heightened US scrutiny of Arabian Gulf wealth funds and their ties to China. The divide between the two ecosystems is the live outcome of a contest between Arabian Gulf incentives to diversify across both and US policy pressure to force a choice, and that contest is unresolved, since Arabian Gulf capital is present on the Chinese side now.

Two caveats should travel with this finding. The first concerns scope. The evidence of two-sided exposure is established specifically for Arabian Gulf capital. It does not extend to Singaporean or Japanese actors, and Korea's appearance through Mirae Asset is a new entry rather than a sovereign actor of the kind the project tracks. The finding also operates at the level of the region rather than the individual fund, since no single named fund is yet confirmed to hold positions in both a US and a Chinese frontier lab. The second caveat concerns what the data can show. The tracker documents that foreign capital is present, but public sources do not reveal what governance rights, if any, accompanied any of these positions, including the Zhipu private round. Presence is established. Influence is not.

Recommendations

The findings point to three areas where AI safety funders and European policymakers can focus near-term work.

The first is to determine why European institutional capital has not engaged frontier AI. The finding above separates two vehicles, and the appropriate work differs for each. For European Union budgetary capital, the constraint is now identified, and the useful contribution is timing. The drafting of the 2028 to 2034 framework, concluding in 2027, is the window in which AI

safety can be argued into the budget as a recognised priority, and a funder such as Astralis is well-placed to support the analysis and convening that would make that case before the window closes. For sovereign wealth funds and pension funds, the barrier is not yet known, and the higher-value contribution is research. Astralis is well-positioned to commission targeted study of how major European institutional investors make decisions about private market and frontier technology exposure, and to facilitate dialogue between those institutions and AI safety researchers who can make the governance case for engagement.

The second is to map the conditions under which equity investment translates into governance influence. The tracker records who has invested and at what scale, but public sources do not reveal what investors have asked for or received in return. Public sources document two forms of influence operating in practice. The first is formal conditionality, illustrated by the requirement that G42 divest its Chinese technology holdings as a condition of Microsoft's investment. The second is informal, illustrated by the July 2025 Anthropic internal memo in which leadership modelled Arabian Gulf capital as a factor shaping strategic decisions.[12] A third form is regulatory and procurement conditionality, and it is worth noting because Europe is actively building tools of this kind. The Industrial Accelerator Act, proposed by the European Commission in March 2026, introduces preferences for European-origin goods in public procurement and conditions on foreign investment in strategic sectors, and the negotiation around it has exposed a fault line between France, which champions the approach, and Germany and others, which resist it as

[12] Reporting on Anthropic's July 2025 internal memo, Wired — https://www.wired.com/story/anthropic-dario-amodei-gulf-state-leaked-memo/

protectionist.[13][14][15][16] That fault line is directly relevant to the middle power coalition dynamics the project examines. One qualification is essential. AI is not within the scope of the Act as proposed, and the Commission cannot add it through a delegated act, so the Act is not itself a lever for AI, and any AI-specific conditionality would require a separate instrument. The most direct way to advance this part of the project is a targeted interview programme with current and former investment staff at sovereign funds and with deal-side staff at the labs.

The third is to treat the US and China investment divide as a contested outcome and to model the contest. The divide is not a structural feature of the landscape. Arabian Gulf capital is present on both sides as a bloc, and the degree of separation between the two ecosystems is shaped by policy. The conditions under which it might widen or narrow, whether through Chinese regulatory opening, Arabian Gulf strategic recalculation, or changes in US export-control and investment-screening policy, are worth modelling now rather than after the fact. Astralis and similar foundations could usefully support research into the geopolitical and regulatory factors that govern foreign investor access to Chinese AI, both to understand the current divide and to anticipate how it might change.

---

[13] Commission proposes Industrial Accelerator Act to strengthen industry and create jobs in Europe — https://ec.europa.eu/commission/presscorner/detail/en/ip_26_515

[14] Industrial Accelerator Act: the EU Commission launches the "Made in Europe" plan — https://www.renewablematter.eu/en/industrial-accelerator-act-eu-commission-launches-made-in-europe-plan

[15] Industrial Accelerator Act: EU's push for 'Made in Europe' — https://ioplus.nl/en/posts/industrial-accelerator-act-eus-push-for-made-in-europe

[16] EU Launches Industrial Accelerator Act to Double Manufacturing Share by 2035 — https://www.trendingtopics.eu/eu-launches-industrial-accelerator-act-to-double-manufacturing-share-by-2035/

ASML Cannot Coerce Washington: A Reciprocal Framework for European AI Access

Giulio Bernasconi

giuliobernasconi2003@gmail.com

Executive Summary

ASML, a Dutch company, is the only producer in the world of EUV lithography machines, the equipment needed to manufacture the leading-edge chips used to train frontier AI models[17]. This makes ASML a chokepoint in the semiconductor supply chain, and thus, in theory, a significant source of leverage for the Netherlands and the EU. In practice, several constraints sharply limit how that leverage can be used.

This paper argues that the Netherlands cannot use ASML to coerce the United States, where major frontier AI companies are based, to comply with its regulations and safety standards. It can, however, use ASML in a different kind of deal: Europe continues to align with US semiconductor export controls, and in exchange, it gains negotiated access to frontier AI models. The argument proceeds in three steps. First, it identifies four reasons why the Netherlands cannot credibly threaten to restrict ASML's exports on its own: American influence inside ASML's corporate governance, US legal reach through the Foreign Direct Product Rule, the risk of US retaliation, and the domestic economic cost of any disruption. Second, it uses these four reasons to derive three criteria that any workable policy must meet: it must not impose heavy costs on ASML, must not disrupt the semiconductor supply chain, and must satisfy proportionality requirements under Dutch and EU law. Third, it tests two candidate policies

[17] Will Hunt and Remco Zwetsloot, "Tracing the Emergence of Extreme Ultraviolet Lithography," Center for Security and Emerging Technology, Georgetown University, December 2020, https://cset.georgetown.edu/publication/tracing-the-emergence-of-extreme-ultraviolet-lithography/

against these criteria and shows that only a reciprocal arrangement backed by a European coalition meets all three.

Introduction & Problem Statement

Europe is lagging behind in access to and regulation of frontier AI models. The recent Mythos release is a clear example of this. On 7 April 2026, Anthropic announced Project Glasswing, a special initiative to release the new Mythos Preview model to a restricted number of stakeholders in the US[18]. Mythos is a new frontier AI model that allegedly has significantly improved cyber capabilities, able to find zero-day vulnerabilities in the most widely used systems, from operating systems to critical finance software[19]. No European stakeholders got access to this model, neither European cybersecurity agencies nor European companies[20]. This lack of access matters in two ways. First, it signals Europe's limited strategic relevance in the frontier AI ecosystem: the most important developers do not necessarily treat European institutions as priority partners when releasing sensitive capabilities. Second, it creates a direct security problem because European states and firms may be exposed to new AI-enabled cyber risks without having the same opportunity as US actors to evaluate, test, or prepare for them[21].

The issue is not just about access but also regulations. Under the AI Act, the EU AI Office is tasked with supervising general-purpose AI models that pose systemic risk[22]. Providers of such models must conduct model evaluations, assess and mitigate systemic risks, report serious incidents, and ensure cybersecurity protections[23]. In addition, the Commission may request information and, where necessary, ask for access to the model through APIs or other

[18] Anthropic, "Project Glasswing: Securing Critical Software for the AI Era," accessed May 11, 2026, https://www.anthropic.com/glasswing

[19]Ibid

[20] Sam Clark, "Europe Craves Its Own Superhacking AI," *POLITICO*, April 27, 2026, https://www.politico.eu/article/europe-craves-its-own-superhacking-ai/.

[21] Reinhard Becker, "EU Should Seek Access to Anthropic's Mythos, Bundesbank Says," *Reuters*, April 29, 2026, https://www.reuters.com/legal/litigation/eu-should-seek-access-anthropics-mythos-bundesbank-says-2026-04-29/

[22] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence, art. 88, *Official Jornalofthe European Union*, July 12, 2024, https://eur-lex.europa.eu/eli/reg/2024/1689/oj. equest

[23] Regulation (EU) 2024/1689, art. 55.

technical means in order to conduct evaluations[24]. In theory, this should give the AI Office a mechanism to examine whether a frontier model with advanced cyber capabilities has been properly tested and whether its risks have been mitigated. In practice, however, the Mythos case suggests that this legal framework does not automatically translate into timely access or operational control. If European authorities are excluded from restricted release programs, they may be able to regulate and evaluate only after the release in the European market, thereby compromising the safety objectives of the AI Act. The Mythos case showed clearly how Europe lacked both access to and control over the most advanced AI model, and even one of the most critical dual-use technologies.

European access and control are critical to ensuring AI is safe because, without European oversight, the US would be motivated mainly by economic incentives and geopolitical dynamics[25], which could lead to extremely negative outcomes[26]. Historically, we have seen how private companies, in the absence of regulations, could support and develop systems that do not protect users. In the absence of strict US regulations, as is currently the case for AI development, having an external oversight and regulatory regime is key to ensuring the technology is developed in accordance with safety protocols and that risks are monitored and mitigated. The EU AI Act framework ensure all of this and can thus significantly decrease the risk associated with AI development. This is also closely related to the European Union's role in AI development and to ensuring the EU's strategic positioning as an influential stakeholder. The question is thus how the EU can strengthen its role to ensure its access to frontier models and the enforcement capabilities for its regulations. Without pre-access to frontier models, EU regulations will lag in enforcement, thereby making safety and EU values an abstract concern rather than an applied, enforced framework.

---

[24] Regulation (EU) 2024/1689, arts. 91–92.

[25] Eoghan Stafford, Robert Trager, and Allan Dafoe, "Safety Not Guaranteed: International Strategic Dynamics of Risky Technology Races," Centre for the Governance of AI, November 1, 2022, https://www.governance.ai/research-paper/safety-not-guaranteed-international-strategic-dynamics-of-risky-technology-races

[26] Markus Anderljung et al., "Frontier AI Regulation: Managing Emerging Risks to Public Safety," *arXiv*, November 7, 2023, https://arxiv.org/abs/2307.03718

This paper argues that the answer runs through ASML. As the only producer of EUV lithography machines in the world, ASML gives the Netherlands, and thus the EU, significant theoretical leverage over the United States. This leverage, however, should not be the opening move. It can instead be repositioned as the implicit collateral of a reciprocal arrangement in which continued European alignment with US semiconductor export controls is exchanged for negotiated access to frontier AI models. By "implicit collateral," I mean that ASML's chokepoint position does not appear as a clause in the proposed agreement and is not deployed as a threat in negotiations. It functions instead as a latent outside option. The shared knowledge that the Netherlands can escalate and exercise control over ASML is what makes US concessions on European AI access durable, and what makes continued European alignment on export controls credible. Coercive use is preserved as an escalation option, not as the initial policy instrument: its function is to make the reciprocal arrangement credible.

Background & Context

One of the key factors influencing the increase in AI capabilities is compute[27]. Compute refers to the aggregate of specialised semiconductor hardware, located in data centres and connected by high-bandwidth networking, used to train and run AI models. From training to deployment, AI models need vast numbers of advanced chips. Producing these chips is extremely complex and requires specialised expertise and substantial R&D investment. This is reflected in the semiconductor supply chain, where a few players dominate.

ASML is an example of that. ASML is a Dutch company based in Veldhoven that produces semiconductor manufacturing equipment[28]. It specialises in lithography machines that print circuit patterns onto silicon wafers. Two main types of these machines are produced: DUV and EUV. Extreme Ultraviolet machines are the main focus of this paper, since they are required to produce the leading-edge nodes (7nm and below) used to manufacture frontier AI chips. There are no other companies in the world capable of producing EUV machines apart from ASML[29].

---

[27] Girish Sastry et al., "Computing Power and the Governance of Artificial Intelligence," *arXiv*, February 2024, https://arxiv.org/abs/2402.08797.

[28] ASML, "About ASML," accessed May 11, 2026, https://www.asml.com/company/about-asml.

[29] ASML, "Busting ASML Myths," February 23, 2022, https://www.asml.com/news/stories/2022/busting-asml-myths.

ASML is widely viewed as a chokepoint in the semiconductor supply chain[30]. While multiple definitions of chokepoints exist, for the purposes of this analysis we follow Rogers (2026), who defines a chokepoint as a highly central node in the AI value chain where demand is relatively inelastic[31]. This definition translates into three clear criteria for identifying a chokepoint asset: few viable substitutes, significant barriers to entry, and difficulty for competitors to bypass through innovation. ASML clearly satisfies all three conditions. Because nearly all advanced AI chips worldwide, with the partial exception of Huawei's recent Ascend 910C, rely on EUV lithography, control over the production and servicing of EUV machines gives the Netherlands and the EU significant theoretical leverage.[32]

Rogers's chokepoint criteria are necessary conditions for leverage, but, as the same paper argues, they are not sufficient[33]. By "leverage" we mean the ability to cut adversaries off from the provision of the goods, thus conferring significant power on the state controlling this specific chokepoint[34]. This power depends on the country's ability to withstand retaliation and undertake the risk of using the company as a coercive tool in negotiations.

The debate over leveraging ASML centers on whether ASML's monopoly translates into real European leverage, or whether the company's dependence on US components negates that monopoly in practice. RAND's recent report highlights how the leverage, clearly evident in ASML's monopoly, is limited by various risks, ranging from US retaliation and dependence to European fragmentation. The conclusion of the report is that "Europe should deploy its leverage in a measured, strategic way to deter economic coercion and to shape a global governance

---

[30] Andre Barbe and Will Hunt, "Preserving the Chokepoints: Reducing the Risks of Offshoring Among U.S. Semiconductor Manufacturing Equipment Firms," Center for Security and Emerging Technology, May 2022, https://doi.org/10.51593/20210045

[31] Dylan Rogers, "Soft Sovereignty: The Limits of Middle Power Leverage and the Semiconductor Supply Chain," SSRN, April 2, 2026, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=6511318.

[32] Maximilian Negele et al., *Europe and the Geopolitics of AGI: The Need for a Preparedness Plan* (Santa Monica, CA, and Cambridge, UK: RAND Corporation and Centre for Future Generations, 2025), 44, https://cfg.eu/wp-content/uploads/Europe-and-the-geopolitics-of-AGI.pdf.

[33] Dylan Rogers, "Soft Sovereignty: The Limits of Middle Power Leverage and the Semiconductor Supply Chain," SSRN, April 2, 2026, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=6511318.

[34] Henry Farrell and Abraham L. Newman, "Weaponized Interdependence: How Global Economic Networks Shape State Coercion," *International Security* 44, no. 1 (Summer 2019): 42–79, https://doi.org/10.1162/isec_a_00351.

regime that protects European interests[35].” The Centre for Future Generations supports this hypothesis, underlining strategic indispensability as the foundation of European strategy. The report claims that “For the EU, holding these global bottlenecks on European soil turns existing strengths into durable geopolitical leverage in an increasingly transactional semiconductor landscape.”[36]

On the other hand, recent academic reports highlight that the risks of leveraging ASML are too high and that this should not be considered a politically feasible policy option. Rogers (2026) interviewed multiple US officials involved in negotiations with the Netherlands over Chinese export controls and states that “the threat that the Dutch would weaponize dependence against the US did not feature in US decision making.”[37] Rogers explained this lack of leverage through the lens of structural power[38], noting that ASML lacks real control over the semiconductor production structure because it is heavily reliant on US exports for key components and software for its machines.

ASML has not been used as leverage by the Netherlands to date. Instead, the United States has, through bilateral negotiations, controlled the company's export-control decisions, restricting exports to Chinese companies[39]. These episodes show that the company has been easily influenced by the US, limiting Dutch and European control.

This paper maps the constraints of using ASML as leverage and examines the underlying reasons for the lack of strategic control over this key company.

---

[35] Maximilian Negele et al., *Europe and the Geopolitics of AGI: The Need for a Preparedness Plan* (Santa Monica, CA, and Cambridge, UK: RAND Corporation and Centre for Future Generations, 2025), 44, https://cfg.eu/wp-content/uploads/Europe-and-the-geopolitics-of-AGI.pdf.

[36] Sam Bogerd and Thomas Van Damme, “Securing Chip Access through Strategic Indispensability,” Centre for Future Generations, January 5, 2026, https://cfg.eu/securing-chip-access-through-strategic-indispensability/.

[37] Dylan Rogers, “Soft Sovereignty: The Limits of Middle Power Leverage and the Semiconductor Supply Chain,” SSRN, April 2, 2026, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=6511318.

[38] Susan Strange, *States and Markets: An Introduction to International Political Economy* (London: Pinter Publishers, 1988), 25.

[39] Chris Miller, Gregory C. Allen, and Emily Benson, “Balancing the Ledger: Export Controls on U.S. Chip Technology to China,” Center for Strategic and International Studies, February 21, 2024, https://www.csis.org/analysis/balancing-ledger-export-controls-us-chip-technology-china.

Analysis

The constraints on using ASML as leverage fall into four categories:

1. American influence embedded in ASML's corporate structure
2. American legal limitations (FDPR) and Dutch Law
3. International retaliation from the US
4. Domestic economic damage

Corporate structure

Three of the people sitting on ASML's corporate governance bodies are American nationals. As a Dutch NV, ASML operates under a two-tier board system: a Board of Management that runs the company day-to-day[40], and a Supervisory Board that oversees strategy, appoints and can suspend executive management, and advises on major decisions[41]. Wayne Allan, an American, sits on the Board of Management as EVP and Chief Strategic Sourcing and Procurement Officer, giving him direct executive responsibility over the supply chain that is central to any export control discussion. On the Supervisory Board, Mark Durcan, former CEO of Micron Technology, chairs the Technology Committee, while Terri Bresenham chairs the Remuneration Committee.

The Supervisory Board does not run operations, so its American members do not directly control what ASML sells or to whom. However, the structural position of these individuals is relevant. The Supervisory Board's power to appoint and remove executive management also creates an indirect channel through which US-aligned interests could, hypothetically, shape who leads the company and how leadership responds to political pressure. Allan's executive position is perhaps the most direct: as the officer responsible for procurement, his role sits at the

[40] ASML, "Board of Management," accessed May 11, 2026, https://www.asml.com/en/company/governance/board-of-management.

[41] ASML, "Supervisory Board," accessed May 11, 2026, https://www.asml.com/en/company/governance/supervisory-board.

intersection of component dependency and export compliance. None of this implies that these individuals act as proxies for Washington, but it does mean that the governance structure is not neutral from a geopolitical standpoint, and that interventions from the Dutch government would encounter American perspectives at multiple levels of the organisation before taking effect.

ASML also has the option of relocating to the US. In early 2024, ASML openly threatened to move parts of its operations abroad, and the Dutch government responded with a €2.7 billion retention package[42]. This exit option gives ASML significant bargaining power against any government seeking to impose obligations it finds unfavorable[43]. At the same time, since all operations are based in Veldhoven, transferring 24,000+ employees[44] and a deep supplier ecosystem seems unrealistic.

ASML's leadership has also shown it is willing to use its public profile to resist Dutch government pressure. Former CEO Peter Wennink called export restrictions "not conducted on the basis of figures or data, but on the basis of ideology"[45] and actively lobbied against them while still in office[46]. This reflects a broader corporate self-image that prioritises commercial neutrality over alignment with state foreign policy objectives.

---

[42] Toby Sterling, "Dutch Will Spend $2.7 Billion on Improving Infrastructure to Keep ASML," *Reuters*, March 28, 2024, https://www.reuters.com/world/europe/dutch-government-launch-plan-keep-asml-netherlands-2024-03-28/.

[43] Ashifa Kassam and agencies, "Dutch Ministers Trying to Stop Tech Firm ASML Moving Abroad over Foreign Labour Fears," *The Guardian*, March 6, 2024, https://www.theguardian.com/world/2024/mar/06/dutch-ministers-trying-to-stop-tech-firm-asml-moving-abroad-over-foreign-labour-fears.

[44] ASML, "Working in the Netherlands," accessed May 19, 2026, https://www.asml.com/en/careers/working-at-asml/netherlands

[45] BNR Webredactie, "Oud-ASML-ceo: 'Chipoorlog tussen VS en China zal nog tientallen jaren duren,'" *BNR*, July 8, 2024, https://www.bnr.nl/nieuws/economie/10551876/oud-asml-ceo-chipoorlog-tussen-vs-en-china-zal-nog-tientallen-jaren-duren.

[46] Lionel Lim, "China Is Still a Decade behind the U.S. in Chip Technology—but the World Still Needs the Mature Chips It's Making, Says ASML's CEO," *Fortune Asia*, July 9, 2024, https://fortune.com/asia/2024/07/09/china-still-decade-behind-us-chip-tech-asml-ceo-christophe-fouquet-peter-wennink/.

American legal limitations (FDPR) and Dutch Law

The Bureau of Industry and Security (BIS) dramatically expanded the FDPR, meaning that foreign-produced semiconductor manufacturing equipment "that contains any amount of U.S.-origin integrated circuits" is subject to U.S. controls[47]. Per this version of the rule, U.S.-origin integrated circuits include any such chips manufactured with U.S. machines.

ASML's apparent independence is undermined by how deeply embedded American technology is in its production chain. Its largest R&D and manufacturing site outside Europe occupies the former Silicon Valley Group campus in Wilton, Connecticut[48], and two of its key subsidiaries, Cymer, which produces the EUV light source[49], and HMI, which develops e-beam metrology tools, are both based in California[50]. The chip designs that run through its machines rely on electronic design automation software dominated by US firms Synopsys and Cadence. The dependency runs all the way down[51]. Any European attempt to deploy ASML as an autonomous geopolitical instrument therefore encounters a prior constraint: the US holds structural leverage over the technology stack ASML depends on[52].

---

[47] Gregory C. Allen, "Understanding the Biden Administration's Updated Export Controls," Center for Strategic and International Studies, December 11, 2024, https://www.csis.org/analysis/understanding-biden-administrations-updated-export-controls.

[48] Kate Brunton, "7 Things You Didn't Know about ASML's History in Wilton, Connecticut," ASML, October 11, 2023, https://www.asml.com/en/news/stories/2023/seven-things-about-our-wilton-history.

[49] ASML, "ASML to Acquire Cymer to Accelerate Development of EUV Technology," press release, October 17, 2012, https://www.asml.com/en/news/press-releases/2012/asml-to-acquire-cymer-to-accelerate-development-of-euv-technology.

[50] ASML, "ASML to Acquire HMI to Enhance Holistic Lithography Product Portfolio," press release, June 16, 2016, https://www.asml.com/en/news/press-releases/2016/asml-to-acquire-hmi-to-enhance-holistic-lithography-product-portfolio.

[51] Calvin Zeng and Chris Zeoli, "Synopsys and Cadence: The $160B Unsung Giants of Semiconductor Design," *Data Gravity*, April 18, 2024, https://www.datagravity.dev/p/synopsys-and-cadence-the-160b-unsung.

[52] Dylan Rogers, "Challenges to Chokepoints: Does Controlling ASML Really Get You Leverage?," *Features and Targets*, March 18, 2026, https://featuresandtargets.substack.com/p/challenges-to-chokepoints.

The US can thus influence ASML export controls through legal pressure[53]. In practice, FDPR has been used as a threat: the reasoning was that if the Dutch government did not align its export controls with the US entity list, the US would impose them directly through FDPR.

It is, however, important to note that, while not respecting FDPR controls would clearly result in a violation of US law, increasing export controls on ASML machines to a higher threshold would not violate FDPR. The Dutch government could thus adopt stricter rules, targeting, for example, Dutch personnel abroad or sales to dangerous actors not on the US entity list. FDPR is a floor rather than a ceiling for export controls. It is also worth noting that certain legal scholars argue that FDPR export controls are an overreach beyond the permissible boundaries of international law, meaning their long-term enforceability may itself be contested[54].

Beyond FDPR, any intervention by the Dutch government in ASML's operations must satisfy a proportionality requirement under both Dutch administrative law (the Algemene wet bestuursrecht)[55] and the EU Charter of Fundamental Rights[56]. Interference with a private company requires a legitimate public aim and must be no more restrictive than necessary. This constraint matters most for the more intrusive types of intervention: requiring preferential model access is on solid legal footing, but forcing contract termination or restricting Dutch engineers from working abroad would require a much stronger and more specific legal basis.

International retaliation

Given the strategic importance of EUV machines, any action that goes against US interests risks triggering retaliation against the Netherlands and Europe. The US has demonstrated its

---

[53] Rebecca Christie, "US Threat Gives ASML New Headache on China Exports," *Reuters Breakingviews*, June 30, 2023, https://www.reuters.com/breakingviews/us-threat-gives-asml-new-headache-china-exports-2023-06-30/.

[54] Daan Kingma, "Caught in a Geopolitical Crossfire: Questioning the Legality of US-Imposed Export Controls on Dutch Computer Chip Machines," *EJIL: Talk!*, January 12, 2024, https://www.ejiltalk.org/caught-in-a-geopolitical-crossfire-questioning-the-legality-of-us-imposed-export-controls-on-dutch-computer-chip-machines/.

[55] Netherlands, *Algemene wet bestuursrecht* [General Administrative Law Act], art. 3:4(2), https://wetten.overheid.nl/BWBR0005537/.

[56] Charter of Fundamental Rights of the European Union, art. 52(1), 2012 O.J. C 326/391, https://fra.europa.eu/en/eu-charter/article/52-scope-and-interpretation-rights-and-principles.

willingness to use legal and political coercion to enforce alignment: in 2023, Washington explicitly threatened to invoke FDPR unilaterally to restrict ASML's servicing operations in China if the Dutch government did not act[57]. The CHIPS Act also conditions certain benefits on recipient companies aligning with US export control objectives, which gives Washington additional leverage in negotiations[58].

More speculative but not implausible retaliation scenarios could include the blacklisting of Dutch companies or pressure on trade agreements. The withdrawal of NATO commitments is sometimes mentioned but is at the extreme end of what is realistically foreseeable given the broader security relationship.

There is a scenario in which US companies that provide necessary components for ASML machines would be blocked from selling those components. However, this seems extremely unlikely since a full stop in production of ASML machines would have severe consequences for financial markets worldwide, including in the US[59]. The mutual dependence here acts as a restraint on escalation.

Economic damage

ASML reported €32.7 billion in total net sales for 2025[60]. Combined with its workforce and critical role in global supply chains, this makes it a strategic asset for the Netherlands. Any policy intervention, such as licensing obligations or stricter export controls, would likely result in

[57] Rebecca Christie, "US Threat Gives ASML New Headache on China Exports," *Reuters Breakingviews*, June 30, 2023, https://www.reuters.com/breakingviews/us-threat-gives-asml-new-headache-china-exports-2023-06-30/.

[58] Sujai Shivakumar, Charles Wessner, and Thomas Howell, "'Guardrails' on CHIPS Act Funding to Restrict Investments in China May Restrict Participation in CHIPS Act Incentives," Center for Strategic and International Studies, November 7, 2023, https://www.csis.org/blogs/perspectives-innovation/guardrails-chips-act-funding-restrict-investments-china-may-restrict.

[59] Antoine Haramboure, Marcel Rudolfsen, and Łukasz Rawdanowicz, "Vulnerabilities in the Semiconductor Supply Chain," OECD Science, Technology and Industry Working Papers, no. 2023/05, OECD Publishing, 2023, https://www.oecd.org/en/publications/vulnerabilities-in-the-semiconductor-supply-chain_6bed616f-en.html.

[60] ASML, "ASML Reports €32.7 Billion Total Net Sales and €9.6 Billion Net Income in 2025," press release, January 28, 2026, https://www.asml.com/news/press-releases/2026/q4-2025-financial-results.

a loss of revenue and carry real economic costs for the country. A more pessimistic scenario with economic retaliation from the US could lead to a significant economic crisis given the current role of semiconductor supply chains in financial markets. This does not make intervention impossible, but it raises the political bar for action and creates domestic opposition from business and financial stakeholders with a direct interest in ASML's commercial performance.

Recommendations

The constraints mapped in the previous analysis translate into three operational criteria for any policy instrument seeking to leverage ASML's role.

1. First, the economic impact on ASML itself must be low. The company has shown a credible exit option and a history of resisting political pressure through public statements. Moreover, the company is a key strategic asset for the Dutch economy. Any instrument that imposes large costs on ASML will therefore be politically fragile.

2. Second, the instrument must avoid disrupting the semiconductor supply chain. ASML's dependence on American components means that any direct regulation over shipments, servicing, or US-origin content can quickly become a fight over FDPR and the broader ecosystem of American export controls.

3. Third, the intervention must remain proportionate under Dutch administrative law and the EU Charter of Fundamental Rights. The more intrusive the intervention into ASML's commercial freedom, the stronger the legal basis required to justify it.

Together, these criteria define the filter for the different policy instruments considered.

Defining the objective

A reasonable set of objectives, based on the previous criteria, includes the following:

- Preferential access to frontier AI models[61], primarily for European public-sector and cybersecurity agencies. This could mean privileged API terms, bounded deployment rights, secure access through approved cloud environments, or access to restricted model classes for national cybersecurity agencies, ENISA, CERT-EU, and other trusted public bodies. The recent Mythos case is a good illustration of how access could have had a concrete defensive value from which Europe could have benefited[62].

- Pre-release evaluation and red-team access for the EU AI Office and competent member-state authorities. This would give European regulators earlier and more substantive visibility into frontier systems, allowing more effective evaluation by the European institutions in charge of EU AI Act enforcement.

- Service-continuity guarantees in a crisis scenario, so European public agencies are not cut off from American model providers during an export-control or national-security dispute.

Candidate instruments

The next step is to examine candidate policy instruments. Two instruments are worth evaluating.

The first is a reciprocal access arrangement. It would be modelled on the emerging pattern of US technology and AI agreements with selected partners, such as the Pax Silica coalition[63]. In this instrument, the Netherlands and the EU would link continued alignment with US semiconductor export controls to negotiated European access to frontier AI models. ASML itself would not be the regulatory instrument, but the implicit collateral in the agreement. The

[61] Anton Leicht and Dean Ball, "The Race Worth Winning: Middle Powers in the Age of Machine Intelligence," Foundation for American Innovation, February 13, 2026, https://www.thefai.org/posts/the-race-worth-winning-middle-powers-in-the-age-of-machine-intelligence.

[62] Sam Clark, "Europe Craves Its Own Superhacking AI," *POLITICO*, April 27, 2026, https://www.politico.eu/article/europe-craves-its-own-superhacking-ai/.

[63] U.S. Department of State, "Pax Silica Summit," December 11, 2025, https://www.state.gov/releases/office-of-the-spokesperson/2025/12/pax-silica-initiative.

instrument does not impact ASML but supports a mutually beneficial relationship between the EU and the US.

The second is a dual-use regulation pathway, built on Regulation (EU) 2021/821[64]. The Netherlands has used this route for advanced semiconductor manufacturing equipment. The Commission's 2025 update to Annex I also brought additional semiconductor manufacturing and testing equipment into the EU control list. Under this framework, competent authorities have audit and inspection rights over the machines. However, this would only apply to ASML machines, since the EU lacks a framework similar to the American FDPR. Developing a new legal basis for such an export framework could be an important research direction.

The two options differ on the three criteria. Option 1 satisfies all of them: ASML is not directly regulated, the semiconductor supply chain is not disrupted, and a voluntary reciprocal arrangement does not raise proportionality concerns. Option 2 is weaker on the first two. Audit, inspection, or licensing obligations under Regulation 2021/821 create compliance costs for ASML and risk collision with FDPR. Both options satisfy the proportionality criterion, since the dual-use route has clear legal grounding. Option 1 is thus the recommended primary instrument, while Option 2 remains a useful complementary tool that can be activated as part of the escalation ladder described below.

Coalition logic and the retaliation question

The decisive political factor in predicting the effectiveness of such a policy is whether the Netherlands acts alone or under European cover. The previous analysis made clear that a Dutch-only play is not credible, since the asymmetry in economic exposure between the Netherlands and the United States is too large. The question is whether a European or multi-state framing actually changes that calculation.

[64] Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items, *Official Journal of the European Union* L 206, June 11, 2021, 1–461, https://eur-lex.europa.eu/eli/reg/2021/821/oj.

A European coalition is thus needed to effectively leverage the strategic role of ASML[65]. A possible coalition may be composed of the Netherlands and Germany because of their key role in the semiconductor supply chain with ASML, Zeiss, and Trumpf[66]. Other countries, such as France, could align since this coalition clearly supports an already "popular" framing of strategic European autonomy. Other European countries, such as Belgium, Italy, or Nordic states, could join since this represents the most concrete option to ensure model-access and cyber-defence concessions. This coalition would not be a "favour" to the Netherlands but rather a strategic coalition that brings concrete benefits to its partners, benefits that could not have been obtained otherwise.

To make any of this credible, a clear escalation strategy needs to be developed. Even if a bilateral agreement with the United States is the preferred outcome, an escalation strategy is needed to make this proposal credible. A possible plan would include different tiers, starting from linkage to other EU-US negotiation tracks, escalating to activation of EU dual-use review under Regulation 2021/821, and, as a more extreme option, servicing restrictions on ASML machines[67]. Concessions would be extracted at the lower tiers precisely because the higher tiers remain credible. This paper does not recommend these "extreme" strategies, but argues that a concrete escalation ladder is needed for a credible approach. The assumption is that an escalation would be extremely negative for both partners. Key US tech firms such as NVIDIA, Apple, and Qualcomm are all deeply dependent on TSMC and ASML machines, and severe escalation would create significant exposure for the US economy as well as for the European one. The ceiling on retaliation would thus be set by American self-interest.

---

[65] Maximilian Negele et al., *Europe and the Geopolitics of AGI: The Need for a Preparedness Plan* (Santa Monica, CA, and Cambridge, UK: RAND Corporation and Centre for Future Generations, 2025), 44, https://cfg.eu/wp-content/uploads/Europe-and-the-geopolitics-of-AGI.pdf.

[66] ASML, "Lenses and Mirrors," accessed May 11, 2026, https://www.asml.com/technology/lithography-principles/lenses-and-mirrors.

[67] Toby Sterling, "ASML Needs Licence to Service Some Equipment in China, Dutch Government Says," *Reuters*, September 10, 2024, https://www.reuters.com/technology/asml-needs-licence-service-some-equipment-china-dutch-government-says-2024-09-10/.

Conclusion

Europe is lagging behind in access to and regulation of frontier AI models, as the Mythos case made clear. ASML is a strong European leverage point in the semiconductor supply chain, but the constraints mapped in this paper, corporate-structural, legal, retaliatory, and economic, rule out its use as a primary coercive instrument. The Netherlands, acting alone, cannot bear the risk of retaliation, and direct intervention in ASML's operations runs into FDPR, proportionality limits, and the company's own exit options.

The same chokepoint position can, however, be repositioned as the implicit collateral of a reciprocal arrangement: continued European alignment with US semiconductor export controls in exchange for preferential model access, pre-release evaluation rights for the EU AI Office, and service-continuity guarantees. This proposal only works under a coalition framing, anchored in Germany's parallel exposure, and backed by a credible escalation ladder. The next research step is the legal design of an EU-level export framework comparable to the American FDPR, which is currently the missing piece to ensure a credible escalation strategy.

References

Allen, Gregory C. “Understanding the Biden Administration’s Updated Export Controls.” Center for Strategic and International Studies, December 11, 2024. https://www.csis.org/analysis/understanding-biden-administrations-updated-export-controls.

Anthropic. “Project Glasswing: Securing Critical Software for the AI Era.” Accessed May 11, 2026. https://www.anthropic.com/glasswing.

ASML. “About ASML.” Accessed May 11, 2026. https://www.asml.com/company/about-asml.

ASML. “ASML Reports €32.7 Billion Total Net Sales and €9.6 Billion Net Income in 2025.” Press release, January 28, 2026. https://www.asml.com/news/press-releases/2026/q4-2025-financial-results.

ASML. “ASML to Acquire Cymer to Accelerate Development of EUV Technology.” Press release, October 17, 2012. https://www.asml.com/en/news/press-releases/2012/asml-to-acquire-cymer-to-accelerate-development-of-euv-technology.

ASML. “ASML to Acquire HMI to Enhance Holistic Lithography Product Portfolio.” Press release, June 16, 2016. https://www.asml.com/en/news/press-releases/2016/asml-to-acquire-hmi-to-enhance-holistic-lithography-product-portfolio.

ASML. “Board of Management.” Accessed May 11, 2026. https://www.asml.com/en/company/governance/board-of-management.

ASML. “Busting ASML Myths.” February 23, 2022. https://www.asml.com/news/stories/2022/busting-asml-myths.

ASML. “Lenses and Mirrors.” Accessed May 11, 2026. https://www.asml.com/technology/lithography-principles/lenses-and-mirrors.

ASML. “Supervisory Board.” Accessed May 11, 2026. https://www.asml.com/en/company/governance/supervisory-board.

Barbe, Andre, and Will Hunt. “Preserving the Chokepoints: Reducing the Risks of Offshoring Among U.S. Semiconductor Manufacturing Equipment Firms.” Center for Security and Emerging Technology, May 2022. https://doi.org/10.51593/20210045.

BNR Webredactie. “Oud-ASML-ceo: ‘Chipoorlog tussen VS en China zal nog tientallen jaren duren.’” BNR, July 8, 2024. https://www.bnr.nl/nieuws/economie/10551876/oud-asml-ceo-chipoorlog-tussen-vs-en-china-zal-nog-tientallen-jaren-duren.

Bogerd, Sam, and Thomas Van Damme. “Securing Chip Access through Strategic Indispensability.” Centre for Future Generations, January 5, 2026. https://cfg.eu/securing-chip-access-through-strategic-indispensability/.

Brunton, Kate. “7 Things You Didn’t Know about ASML’s History in Wilton, Connecticut.” ASML, October 11, 2023. https://www.asml.com/en/news/stories/2023/seven-things-about-our-wilton-history.

Charter of Fundamental Rights of the European Union, art. 52(1), 2012 O.J. C 326/391. https://fra.europa.eu/en/eu-charter/article/52-scope-and-interpretation-rights-and-principles.

Christie, Rebecca. “US Threat Gives ASML New Headache on China Exports.” Reuters Breakingviews, June 30, 2023. https://www.reuters.com/breakingviews/us-threat-gives-asml-new-headache-china-exports-2023-06-30/.

Clark, Sam. “Europe Craves Its Own Superhacking AI.” POLITICO, April 27, 2026. https://www.politico.eu/article/europe-craves-its-own-superhacking-ai/.

Farrell, Henry, and Abraham L. Newman. “Weaponized Interdependence: How Global Economic Networks Shape State Coercion.” International Security 44, no. 1 (Summer 2019): 42–79. https://doi.org/10.1162/isec_a_00351.

Haramboure, Antoine, Marcel Rudolfsen, and Łukasz Rawdanowicz. “Vulnerabilities in the Semiconductor Supply Chain.” OECD Science, Technology and Industry Working Papers, no. 2023/05. OECD Publishing, 2023. https://www.oecd.org/en/publications/vulnerabilities-in-the-semiconductor-supply-chain_6bed616f-en.html.

Hunt, Will, and Remco Zwetsloot. “Tracing the Emergence of Extreme Ultraviolet Lithography.” Center for Security and Emerging Technology, Georgetown University, December 2020. https://cset.georgetown.edu/publication/tracing-the-emergence-of-extreme-ultraviolet-lithography/.

Kassam, Ashifa. “Dutch Ministers Trying to Stop Tech Firm ASML Moving Abroad over Foreign Labour Fears.” The Guardian, March 6, 2024. https://www.theguardian.com/world/2024/mar/06/dutch-ministers-trying-to-stop-tech-firm-asml-moving-abroad-over-foreign-labour-fears.

Kingma, Daan. “Caught in a Geopolitical Crossfire: Questioning the Legality of US-Imposed Export Controls on Dutch Computer Chip Machines.” EJIL: Talk!, January 12, 2024. https://www.ejiltalk.org/caught-in-a-geopolitical-crossfire-questioning-the-legality-of-us-imposed-export-controls-on-dutch-computer-chip-machines/.

Leicht, Anton, and Dean Ball. “The Race Worth Winning: Middle Powers in the Age of Machine Intelligence.” Foundation for American Innovation, February 13, 2026. https://www.thefai.org/posts/the-race-worth-winning-middle-powers-in-the-age-of-machine-intelligence.

Lim, Lionel. “China Is Still a Decade behind the U.S. in Chip Technology—but the World Still Needs the Mature Chips It’s Making, Says ASML’s CEO.” Fortune Asia, July 9, 2024. https://fortune.com/asia/2024/07/09/china-still-decade-behind-us-chip-tech-asml-ceo-christophe-fouquet-peter-wennink/.

Miller, Chris, Gregory C. Allen, and Emily Benson. “Balancing the Ledger: Export Controls on U.S. Chip Technology to China.” Center for Strategic and International Studies, February 21, 2024. https://www.csis.org/analysis/balancing-ledger-export-controls-us-chip-technology-china.

Negele, Maximilian, et al. Europe and the Geopolitics of AGI: The Need for a Preparedness Plan. Santa Monica, CA, and Cambridge, UK: RAND Corporation and Centre for Future Generations, 2025. https://cfg.eu/wp-content/uploads/Europe-and-the-geopolitics-of-AGI.pdf.

Netherlands. Algemene wet bestuursrecht [General Administrative Law Act], art. 3:4(2). https://wetten.overheid.nl/BWBR0005537/.

Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items. Official Journal of the European Union L 206, June 11, 2021, 1–461. https://eur-lex.europa.eu/eli/reg/2021/821/oj.

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence. Official Journal of the European Union, July 12, 2024. https://eur-lex.europa.eu/eli/reg/2024/1689/oj.

Rogers, Dylan. “Challenges to Chokepoints: Does Controlling ASML Really Get You Leverage?” Features and Targets, March 18, 2026. https://featuresandtargets.substack.com/p/challenges-to-chokepoints.

Rogers, Dylan. “Soft Sovereignty: The Limits of Middle Power Leverage and the Semiconductor Supply Chain.” SSRN, April 2, 2026. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=6511318.

Sastry, Girish, et al. “Computing Power and the Governance of Artificial Intelligence.” arXiv, February 2024. https://arxiv.org/abs/2402.08797.

Shivakumar, Sujai, Charles Wessner, and Thomas Howell. “‘Guardrails’ on CHIPS Act Funding to Restrict Investments in China May Restrict Participation in CHIPS Act Incentives.”

Center for Strategic and International Studies, November 7, 2023. https://www.csis.org/blogs/perspectives-innovation/guardrails-chips-act-funding-restrict-investments-china-may-restrict.

Sterling, Toby. "ASML Needs Licence to Service Some Equipment in China, Dutch Government Says." Reuters, September 10, 2024. https://www.reuters.com/technology/asml-needs-licence-service-some-equipment-china-dutch-government-says-2024-09-10/.

Sterling, Toby. "Dutch Will Spend $2.7 Billion on Improving Infrastructure to Keep ASML." Reuters, March 28, 2024. https://www.reuters.com/world/europe/dutch-government-launch-plan-keep-asml-netherlands-2024-03-28/.

Strange, Susan. States and Markets: An Introduction to International Political Economy. London: Pinter Publishers, 1988.

U.S. Department of State. "Pax Silica Summit." December 11, 2025. https://www.state.gov/releases/office-of-the-spokesperson/2025/12/pax-silica-initiative.

Zeng, Calvin, and Chris Zeoli. "Synopsys and Cadence: The $160B Unsung Giants of Semiconductor Design." Data Gravity, April 18, 2024. https://www.datagravity.dev/p/synopsys-and-cadence-the-160b-unsung.

POLICY BRIEF 1

Middle Power Levers

A Taxonomy of Levers for Foreign Governments to Influence the U.S.

Barbara Marchiori de Assis | SPAR Fellowship | May 2026

Introduction

States beyond the dominant AI powers can deploy a range of mechanisms to influence US and global technology governance policy. This brief systematically maps these mechanisms, providing policymakers, advocates, and researchers with a shared analytical vocabulary for understanding how governance influence operates. It presents a three-layer taxonomy of 14 such mechanisms, developed through an iterative empirical-conceptual method grounded in international relations theory and confirmed by evidence from cybersecurity and AI governance practice across 15 countries.

The taxonomy is designed as a practical tool — a structured reference that practitioners, policymakers, and advocates can use to identify which mechanisms are available, how they operate, and what resources they require. It is organized around the directness towards US policy: whether a mechanism targets US decision-makers directly, or operates on the international environment in which US policy is made.

The 15-Country Set

The taxonomy was applied to evidence drawn from Singapore, South Korea, the UAE, Saudi Arabia, Israel, India, France, Japan, the UK, Canada, Brazil, Mexico, Kenya, South Africa, and Nigeria —a set chosen to capture diverse influence strategies across regions, resource levels, and governance traditions.

Two Pathways of Influence

All 14 mechanisms operate through one of two pathways, which differ in timescale, resource requirements, and the type of policy effect they produce.

DIRECT PATHWAY

Mechanisms that engage US decision-making processes explicitly and proximately: lobbying of Congress and executive agencies, formal submissions to NIST rulemaking processes, bilateral treaty and co-governance arrangements, and executive-level diplomatic engagement. Effects on US policy are traceable in legislative records, regulatory dockets, and published bilateral instruments.

Requires Washington access infrastructure: lobbying firms, bilateral diplomatic relationships, and English-language engagement with US regulatory processes.

INDIRECT / GLOBAL PATHWAY

Mechanisms that operate primarily on the international environment in which US policy operates, rather than on US decision-makers directly. This includes multilateral forum convening, epistemic framing through international processes, and capacity-building programs that export governance models to third-country governments, thereby shaping the positions those countries bring to negotiations in which the US is also present.

Requires multilateral positioning, patient institutional investment, and coalition-building capacity.

These two pathways are analytically distinct and produce different types of policy effects. Direct mechanisms are faster and more traceable; indirect mechanisms are slower but can lock in normative gains that are harder to reverse.

Great powers require middle powers for procedural legitimacy, coalition credibility, infrastructure access, and vote margins — and states have learned to convert that indispensability into governance influence.

Methodology

The taxonomy follows the methodology proposed by Sangupamba Mwilu, Prat, and Comyn-Wattiau (2015), adapting Nickerson et al.'s (2013) taxonomy development method to domains where the conceptual body of knowledge is still forming. The development process combines conceptual-to-empirical and empirical-to-conceptual iterations, allowing theoretical frameworks and empirical evidence to inform each other throughout the research process.

The starting point is a meta-characteristic — the most comprehensive characteristic from which each mechanism follows as a logical consequence:

> *The mechanism by which a foreign government exercises influence over US or multilateral governance policy, differentiated by the directness of the causal chain to US policy output.*

The two-pathway structure draws on three theoretical foundations:

- Keohane & Nye (2011): under conditions of complex interdependence, states interact through multiple channels simultaneously — interstate, transgovernmental, and transnational — and international organizations function as particularly accessible instruments for smaller states.
- Cooper (1997): middle powers concentrate diplomatic activity on selected niches where they hold comparative institutional or informational advantages.
- Büthe & Mattli (2011): influence in international standard-setting is a function of informational advantage, not economic power — structurally open to middle powers.

Empirical grounding for Layers B and C draws primarily on Freeman & Cleveland-Stout (2024, Quincy Institute Brief No. 59), which documents FARA-registered foreign lobbying activity across 2022–23.

Why Cybersecurity and AI Governance?

The taxonomy was developed using evidence from both cybersecurity and AI governance because the two domains share four structural features that make cybersecurity an instructive empirical reference:

- Both are dual-use technologies: the same capabilities designed for beneficial or defensive purposes can be repurposed for harm, and this dynamic runs in both directions. Civilian tools can migrate into military and adversarial contexts, while military-grade capabilities find their way into non-conflict settings, creating governance challenges that are simultaneously technical, political, and ethical.
- Both spread through decentralized infrastructure that no single state or institution can fully control, which is why governance in each domain has evolved toward multi-stakeholder arrangements involving governments, private sector actors, technical standards bodies, and civil society.
- Both generate transnational collateral effects: an attack, a system failure, or a governance gap originating in one jurisdiction can propagate across borders in ways that are difficult to trace and harder to contain, making unilateral governance structurally inadequate.
- Both are characterized by a pace of technological change that consistently outstrips the institutional capacity to respond — distinguishing them from governance domains such as aviation or nuclear, where the pace of innovation had largely stabilized before governance architecture matured.

These shared features make the taxonomy applicable across both domains, and what would make it applicable to other domains, such as semiconductors, biotechnology, and quantum computing that exhibit the same structural characteristics. The dual-use feature is particularly

significant: given that civilian and military applications are inseparable in both domains, governance cannot be purely state-led. Private-sector actors — frontier AI labs, infrastructure companies, standards bodies — become both governance participants and targets of influence, which is why the taxonomy includes private-sector & civil-society-facing mechanisms alongside government-facing ones.

[68]Mapping the Mechanisms: Two Axes of Influence

The 14 mechanisms can be mapped on two analytical dimensions. The horizontal axis distinguishes between mechanisms that engage US decision-makers directly and those that operate in the international environment in which US policy is made. The vertical axis distinguishes between mechanisms whose primary targets are government actors and official processes —the US Congress, executive agencies, and multilateral forums— and those whose primary targets are private-sector and civil-society actors: US companies, media, academic institutions, and expert communities. In both cases, the actor deploying the mechanism is always a middle-power government; what varies is the channel through which influence is sought and the type of actor being engaged.

	INDIRECT / GLOBAL **Shapes the international environment**	**DIRECT / US-FACING** **Engages US decision-makers**
GOVERNMENT-FACING *(State actors & official processes)*	**QUADRANT I — Indirect + Government-facing** *Shapes multilateral norms and institutional architecture that the US government must subsequently engage.* ● A3.1 Multilateral forum convening & procedural leadership ● A3.2 Proposing alternative multilateral institutional framework ● A2.1 Security alignment leverage	**QUADRANT II — Direct + Government-facing** *Directly targets US legislative, executive, and treaty processes through lobbying, diplomacy, and bilateral instruments.* ● B1.1 FARA-registered lobbying ● B1.2 NDAA provision embedding ● B2.1 Executive agency & rulemaking engagement ● A1.2 Trade-embedded technology provisions
PRIVATE SECTOR & CIVIL SOCIETY-FACING *(Companies, expert communities, public opinion)*	**QUADRANT III — Indirect + Private Sector & Civil Society-facing** *Shapes normative vocabulary, expert knowledge base, and governance models that reach US policy through non-governmental channels.* ● A1.1 Infrastructure investment & strategic hosting ● A3.3 Epistemic framing of risk & governance vocabulary ● A4.1 Capacity-building & institutional diffusion	**QUADRANT IV — Direct + Private Sector & Civil Society-facing** *Targets US private sector actors, media, academic institutions, and personal access networks that shape the policy environment.* ● B3.1 Academic & think tank influence ● C1 Campaign contributions (amplifier) ● C2 Revolving door hiring (amplifier) ● C3 Social access events (amplifier)

Figure 1: Mechanisms mapped by pathway (direct/indirect) and target (government-facing/private sector & civil society-facing). Layer A mechanisms appear in Quadrants I, II, and III; Layer B and C mechanisms appear in Quadrants II and IV.

68

The Taxonomy of Foreign Government Influence Mechanisms

The taxonomy organizes 14 mechanisms across three layers. Layer A captures upstream mechanisms operating at the international level. Layer B captures direct Washington-facing channels. Layer C captures the financial and relationship-based tools that amplify Layer B's effectiveness.

ID	Mechanism	Description	Selected Examples	Pathway
LAYER A — STRUCTURAL LEVERAGE | Mechanisms operating at the international and multilateral level, shaping the global environment in which US policy is made				
A1 — Economic Leverage				
A1.1	**Infrastructure investment & strategic hosting**	Foreign government-linked firms make large investments in US AI/tech infrastructure or position their countries as indispensable hosts of US compute capacity, creating strategic dependence that generates political access and shapes national security relationships.	**AI:** MGX, an Abu Dhabi sovereign-wealth-backed investment vehicle, co-launched the Global AI Infrastructure Investment Partnership (GAIIP) with BlackRock, Microsoft, and GIP in September 2024, committing $30 billion in equity —primarily for US data centers— with the potential to scale to $100 billion.[69] A UAE-led consortium, including MGX, subsequently acquired Aligned Data Centers, a US-based operator with 78 data centers, for $40 billion (2025).[70] In parallel, G42 and OpenAI partnered to build Stargate UAE, positioning the UAE as an indispensable host of US compute capacity.[71]	*Indirect / Global*
A1.2	**Trade-embedded technology cooperation provisions**	Tech-governance cooperation clauses embedded in bilateral or multilateral trade agreements with Foreign governments.	**Cybersecurity:** Canada and Mexico embedded cybersecurity cooperation provisions in USMCA Article 19.15 (2020).[72] The US–Japan Digital Trade Agreement subsequently copied the clause nearly word-for-word.[73]	*Direct*
A2 — Security Leverage				

[69] BlackRock, Global Infrastructure Partners, Microsoft, & MGX. (September 17, 2024). *Global Infrastructure Partners, BlackRock, Microsoft, and MGX Launch New AI Partnership to Invest in Data Centers and Supporting Power Infrastructure*. https://www.global-infra.com/news/global-infrastructure-partners-blackrock-microsoft-and-mgx-launch-new-ai-partnership-to-invest-in-data-centers-and-supporting-power-infrastructure/

[70] Kumar, P. (October 16, 2025). MGX consortium buys $40bn US data centre company. *AGBI*. https://www.agbi.com/tech/2025/10/mgx-consortium-buys-40bn-us-data-centre-company

[71] Malin, C. (May 26, 2025). New US-UAE agreement sure to accelerate G42's US plans. *Middle East AI News*. https://www.middleeastainews.com/p/us-uae-ai-partnership-g42-us-plans

[72] Office of the U.S. Trade Representative – USTR (2020). USMCA, Chapter 19: Digital Trade. Retrieved from https://ustr.gov/sites/default/files/files/agreements/FTA/USMCA/Text/19-Digital-Trade.pdf

[73] Chang, L. Y-C., and Liu, H-W. (November 2022). "Chapter 8: Ensuring Cybersecurity for Digital Services Trade". In Asian Development Bank (ADB) *Unlocking the potential of Digital Services Trade in Asia and the Pacific*. p. 194. Retrieved from https://www.adb.org/sites/default/files/publication/842321/digital-services-trade-asia-pacific.pdf a credible intent to redirect security partnerships to rival states — in exchange for access to technology

—or signal credible intent to redirect security partnerships to rival states—in exchange for access to technology

A2.1	**Security alignment leverage**	Foreign governments offer or withhold bilateral security cooperation —or signal credible intent to redirect security partnerships to rival states— in exchange for technology access or favorable regulatory treatment.	**AI:** UAE's G42 divested from Huawei and Chinese technology partners in exchange for US AI chip access and the Microsoft $1.5B deal.[74] Saudi Arabia's chip approvals for HUMAIN followed Crown Prince MBS's Washington visit, bundled with F-35 sales and a major non-NATO ally designation.[75]	*Direct*
A3 — Multilateral Positioning				
A3.1	**Multilateral forum convening & procedural leadership**	Foreign governments launch, chair, or shape the agendas of multilateral governance forums, using procedural tools to embed preferred normative vocabulary and institutional models into international frameworks that	**Cybersecurity:** Singapore chaired the UN OEWG on ICT Security (2021–25), deploying the Silence Procedure and cumulative framework language to produce the UN Global Mechanism on Cybersecurity (2025).[76] UK and Singapore co-led the CRI Policy Pillar, producing the first-ever international non-payment of ransoms norm	*Indirect / Global*

[74]Business Standard (reporting on Bloomberg source material), "G42 Made Secret Pact with US to Divest from China Before Microsoft Deal," April 16, 2024, https://www.business-standard.com/world-news/g42-made-secret-pact-with-us-to-divest-from-china-before-microsoft-deal-124041600274_1.html (reporting that US BIS officials, with NSC blessing, told G42 executives they would have to choose between the US or China, and that divestment from Chinese companies was exchanged for assurance of continued US technology access); Fortune, "UAE-Based G42 Cuts Ties with China over US Security Risks," December 7, 2023, https://fortune.com/2023/12/07/emirati-ai-company-picks-side-against-china-g24-us-sanctions/ (confirming G42's pivot to American hardware suppliers to address national security concerns); Times of AI, "UAE's G42 Gets US Approval for AI Chips," November 21, 2025, https://www.timesofai.com/news/uae-g42-gets-us-approval-for-ai-chips/ (confirming Commerce Department authorization of up to 35,000 Nvidia Blackwell-equivalent chips, contingent on rigorous security and reporting requirements under the Regulated Technology Environment framework); CSIS, "The United Arab Emirates' AI Ambitions," January 27, 2025, https://www.csis.org/analysis/united-arab-emirates-ai-ambitions (documenting UAE officials' framing of security cooperation — including space and nuclear collaboration — as evidence justifying upgraded technology access, and their frustration at being categorized alongside countries like Pakistan and Yemen in US export control tiers).

[75]Rest of World, "US Gains in AI Race as Gulf Nations Ditch China for Chips," January 22, 2026, https://restofworld.org/2025/mideast-us-chip-deal-and-china/ (documenting that chip approvals for both G42 and HUMAIN followed divestment pledges from Huawei, and that "Gulf nations turned the US-China rivalry into leverage for their own AI ambitions"); Asia Times, "American AI Chipmakers' Eyes Are on Saudi Arabia Now, Not China," May 23, 2025, https://asiatimes.com/2025/05/american-ai-chipmakers-eyes-are-on-saudi-arabia-now-not-china/ (reporting that Huawei's Ascend chips held approximately 30% market share in Saudi Arabia, primarily through an AI project in NEOM, establishing the credibility of the Chinese alternative); SpaceDaily / AFP, "Saudi AI Firm Humain Inks Nvidia Deal as US Allows Chip Sales," November 20, 2025, https://www.spacedaily.com/afp/251120095616.31axyd62.html (reporting that the Nvidia-HUMAIN deal was announced during Crown Prince MBS's Washington visit, at the same forum where Saudi Arabia also secured a deal to purchase F-35 fighter jets, a civil nuclear energy agreement, and a major non-NATO ally designation); The Soufan Center, "The UAE and KSA's AI Hedge in a Divided Global Order," April 10, 2025, https://thesoufancenter.org/intelbrief-2025-april-10/ (noting that the CEO of Alat, a Saudi state-backed semiconductor investment firm, publicly stated in 2024 that it would divest from Chinese partnerships if they were an issue for the United States, and that both the UAE and KSA face Houthi drone and missile threats that have driven AI-integrated defense investment).

[76] *UN General Assembly (July 2025). Final report of the open-ended working group on security of and in the use of information and communications technologies 2021-2025. Retrieved from https://docs.un.org/en/A/80/257; United Nations General Assembly. (December 2025). Developments in the field of information and telecommunications in the context of international security (Resolution A/RES/80/16). New York: United Nations. Retrieved from https://docs.un.org/en/A/RES/80/16; DigWatch, UN global mechanism on cybersecurity. Retrieved from https://dig.watch/processes/un-gge; Rupp, C. (March 2026). "The UN's New Global Mechanism on Cybersecurity: How Europe Can Advance Responsible State Behavior in Cyberspace." In Interface. Retrieved from https://www.interface-eu.org/publications/the-new-united-nations-mechanism-on-cybersecurity*

		US policy must subsequently engage.	(2023).[77] The Freedom Online Coalition (Canada, France, Japan, Kenya, Mexico, UK) issued a joint statement on the UN Cybercrime Treaty, which the US State Department subsequently joined.[78] ISO/IEC SC 27 outputs were adopted in NIST CSF 2.0.[79] Canada chairs and Brazil vice-chairs the OAS/CICTE Working Group on CBMs in Cyberspace (2025–26).[80]	
A3.2	**Proposing alternative multilateral institutional frameworks**	Foreign governments champion alternative institutional designs for governance to shift negotiating terrain in their favor.	**Cybersecurity:** France, Japan, the UK, and Canada co-sponsored the Programme of Action concept through UNGA resolution (A/RES/77/37). Later, France co-sponsored the establishment of a permanent mechanism	*Indirect / Global*

[77]International Counter Ransomware Initiative 2023 Joint Statement, Retrieved from https://counter-ransomware.org/briefingroom/c86d363c-3d94-4c72-926a-4eceb4a7ec5a; CRI members endorse Guidance to Build Supply Chain Resilience Against Ransomware, Retrieved from https://cyberriskleaders.com/cri-members-endorse-guidance-to-build-supply-chain-resilience-against-ransomware/; Briefing Room Article | International Counter Ransomware Initiative, Retrieved from https://counter-ransomware.org/briefingroom/d9edf4cc-c621-4e98-8c4c-322f96d2159f; White House. (November 2023). *International Counter Ransomware Initiative 2023 Joint Statement*. Retrieved from https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2023/11/01/international-counter-ransomware-initiative-2023-joint-statement/; Cyber Security Agency of Singapore. (October 2025). *Singapore hosted the 5th Counter Ransomware Initiative Summit* [Press release]. PR Newswire. Retrieved from https://www.prnewswire.com/apac/news-releases/singapore-hosted-the-5th-counter-ransomware-initiative-summit-302593856.html; UK Government. (October 2025). *UK leads global fight to stop ransomware attacks on supply chains* [Press release]. GOV.UK. Retrieved from https://www.gov.uk/government/news/uk-leads-global-fight-to-stop-ransomware-attacks-on-supply-chains; Cyber Security Agency of Singapore. (2023, November 2). *International Counter Ransomware Initiative members come together to strongly discourage ransomware payments* [Press release]. Retrieved from https://www.csa.gov.sg/news-events/news-articles/international-counter-ransomware-initiative-members-come-together-to-strongly-discourage-ransomware-payments/

[78]Freedom Online Coalition. (n.d.). Members. Retrieved from https://freedomonlinecoalition.com/members/; Freedom Online Coalition. (n.d.). Joint Statement on the UN Convention Against Cybercrime. Retrieved from https://freedomonlinecoalition.com/joint-statement-on-the-un-convention-against-cybercrime/; U.S. Department of State. (n.d.). The United States Joins Freedom Online Coalition Joint Statement on the United Nations Convention Against Cybercrime. Retrieved from https://2021-2025.state.gov/ and https://2021-2025.state.gov/the-united-states-joins-freedom-online-coalition-joint-statement-on-the-united-nations-convention-against-cybercrime/.

[79]ISO. (n.d.). ISO/IEC JTC 1/SC 27 participation register. https://www.iso.org/committee/45306.html?view=participation; NIST. (n.d.). CSF 2.0 Informative References. https://www.nist.gov/cyberframework/informative-references

[80]OAS, Working Group on Cooperation and Confidence-Building Measures in Cyberspace. Retrieved from https://www.oascybercbms.org/index.php/en-us/

			(A/RES/78/16), which was UNGA-endorsed in December 2025 (A/RES/80/16).[81]	
A3.3	**Epistemic framing of risk & governance vocabulary**	Foreign governments shape the conceptual vocabulary, risk definitions, and normative frames used by US policymakers and in multilateral documents.	**Cybersecurity:** UK/France Pall Mall Process (2024): 'market governance' framing targeting proliferation of commercial cyber intrusion capabilities, subsequently adopted in US State Department joint statements on spyware.[82]	*Indirect / Global*
A4 — Capacity Building				
A4.1	**Exporting governance models through**	Foreign governments fund and deliver cyber/AI governance capacity-building programs in third countries, pre-shaping the institutional architecture and normative vocabulary that those	**Cybersecurity:** Japan funded the ASEAN-Japan Cybersecurity Capacity Building Centre (AJCCBC) in Bangkok (2018–present), training government officials and critical infrastructure operators from all 10 ASEAN member states in cyber defense	*Indirect / Global*

[81] UN Office for Disarmament Affairs – UNODA (2021). *Working Paper for a Programme of Action (PoA) to advance responsible state behavior in the use of ICTs in the context of international security*. Retrieved from https://documents.unoda.org/wp-content/uploads/2021/11/Working-paper-on-the-proposal-for-a-Cyber-PoA.pdf; UN General Assembly (7 December 2022), A/RES/77/37, "Programme of action to advance responsible State behavior in the use of information and communications technologies in the context of international security". Retrieved from https://digitallibrary.un.org/record/3997617?ln=en; UN General Assembly (24 October 2002), A/C.1/77/PV.19, Retrieved from https://docs.un.org/en/A/C.1/77/PV.19; UN General Assembly. (14 November 2022). *Developments in the field of information and telecommunications in the context of international security: report of the 1st Committee: General Assembly, 77th session.* Retrieved from https://digitallibrary.un.org/record/3995343?v=pdf; UN General Assembly. (10 November 2023). *Report of the First Committee: Developments in the field of information and telecommunications in the context of international security* (A/78/404). Retrieved from https://undocs.org/A/78/404; UN General Assembly. (4 December 2023). *Programme of action to advance responsible State behavior in the use of information and communications technologies in the context of international security* (A/RES/78/16). https://undocs.org/A/RES/78/16; UN General Assembly (July 2025). *Final report of the open-ended working group on security of and in the use of information and communications technologies 2021-2025*. Retrieved from https://docs.un.org/en/A/80/257; United Nations General Assembly. (December 2025). *Developments in the field of information and telecommunications in the context of international security* (Resolution A/RES/80/16). New York: United Nations. Retrieved from https://docs.un.org/en/A/RES/80/16; DigWatch, *UN global mechanism on cybersecurity*. Retrieved from https://dig.watch/processes/un-gge; Rupp, C. (March 2026). "The UN's New Global Mechanism on Cybersecurity: How Europe Can Advance Responsible State Behavior in Cyberspace." In *Interface*. Retrieved from https://www.interface-eu.org/publications/the-new-united-nations-mechanism-on-cybersecurity; Delegation of the EU to the UN in New York (September 2025). *UN Member States agree to establish a global mechanism to advance responsible state behavior in cyberspace*. Retrieved from https://www.eeas.europa.eu/delegations/un-new-york/un-member-states-agree-establish-global-mechanism-advance-responsible-state-behaviour-cyberspace_en; Pytlak, A. (August 2025). "Cyber Diplomacy 2.0: From Process to Impact." In *Stimson*. Retrieved from https://www.stimson.org/2025/cyber-diplomacy-2-0-from-process-to-impact/; Pavlova, P. & Painter, C. (August 2025). "The UN's Permanent Process on Cybersecurity Faces an Uphill Battle." In *Lawfare*. Retrieved from https://www.lawfaremedia.org/article/the-un-s-permanent-process-on-cybersecurity-faces-an-uphill-battle.

[82]Foreign, Commonwealth, & Development Office – FCDO (February 2024). *The Pall Mall Process: tackling the proliferation and irresponsible use of commercial cyber intrusion capabilities*. Retrieved from https://www.gov.uk/government/publications/the-pall-mall-process-declaration-tackling-proliferation-and-irresponsible-use-of-commercial-cyber-intrusion-capabilities/the-pall-mall-process-tackling-the-proliferation-and-irresponsible-use-of-commercial-cyber-intrusion-capabilities; US Department of State (September 2024). *Joint Statement on Efforts to Counter the Proliferation and Misuse of Commercial Spyware*. Retrieved from https://2021-2025.state.gov/office-of-the-spokesperson/releases/2024/09/joint-statement-on-efforts-to-counter-the-proliferation-and-misuse-of-commercial-spyware; US Mission to International Organizations in Geneva (October 2024). *US Advances UN Recognition of Threats Posed by Commercial Spyware*. Retrieved from https://geneva.usmission.gov/2024/10/11/u-s-advances-un-recognition-of-threats-posed-by-commercial-spyware/; France Diplomacy (April 2025). *Pall Mall Process: Code of Practice for States to tackle the proliferation and irresponsible use of commercial cyber intrusion capabilities*. Retrieved from https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/news/article/pall-mall-process-code-of-practice-for-states-to-tackle-the-proliferation-and?page_courante=1#pagination_ssra; FCDO (October 2025). *The Pall Mall Process Code of Practice for States*. Retrieved from https://www.gov.uk/government/publications/the-pall-mall-process-code-of-practice-for-states/the-pall-mall-process-code-of-practice-for-states; FCDO (January 2026). *UK and France seek views on commercial cyber intrusion industry practices*. Retrieved from https://www.gov.uk/government/news/uk-and-france-seek-views-on-commercial-cyber-intrusion-industry-practices

	capacity-building programs	countries bring to multilateral forums where the US is also present.	and forensics, exporting Japan's cybersecurity institutional model to countries that subsequently engage in multilateral forums alongside the US.[83]	
LAYER B — WASHINGTON-BASED PROCESS MECHANISMS | Direct institutional channels through which foreign governments engage US decision-makers				
B1 — Direct Legislative Lobbying				
B1.1	**FARA-registered lobbying of Congress & executive agencies**	Foreign governments retain Washington lobbying firms registered under FARA to conduct political outreach and access US decision-makers directly, shaping how the US defines, restricts, and extends access to emerging technologies and the governance frameworks surrounding them.	**AI:** King Abdullah University of Science and Technology (KAUST), a Saudi government-funded research institution, retained Brownstein Hyatt Farber Schreck under FARA to engage US government officials. FARA supplemental statements document Brownstein facilitating direct meetings between KAUST and the Bureau of Industry and Security (BIS) —the agency responsible for AI chip export licensing— including a meeting with the Deputy Assistant Secretary for Export Enforcement (March 18, 2025)[84] and preparation of background materials for a BIS–KAUST meeting (September 22, 2025).[85] The content of those meetings is not disclosed in the filings. Nevertheless, it is noteworthy that Saudi Arabia has been lobbying to be removed from the US AI chip restricted list since the Trump administration took office.[86] **Cybersecurity/AI:** Akin Gump, FARA-registered for the UAE Embassy (Reg. No. 3492), arranged congressional meetings explicitly framed around military and bilateral security relationships in August 2025, while in the same period making separate contacts with Senate offices and NEC/EOP staff on AI cooperation.[87]	*Direct*
B1.2	**NDAA provision embedding**	Foreign governments lobby to embed technology, security assistance, or governance provisions	**Cybersecurity/AI**: AIPAC lobbied Congress throughout early 2025 for the US-Israel Defense Partnership Act (S. 554/H.R. 1229),	*Direct*

[83] Cybil Portal. (January 22, 2025). *ASEAN-Japan Cybersecurity Capacity Building Centre (AJCCBC) – Phase one*. https://cybilportal.org/projects/asean-japan-cybersecurity-capacity-building-centre/

[84] Brownstein Hyatt Farber Schreck, LLP. (2025, September 30). *Supplemental statement pursuant to the Foreign Agents Registration Act, for 6-month period ending August 2025* (Registration No. 5870). US Department of Justice, FARA Registration Unit. https://efile.fara.gov/docs/5870-Supplemental-Statement-20250930-0.pdf

[85] Brownstein Hyatt Farber Schreck, LLP. (2026, March 30). *Supplemental statement pursuant to the Foreign Agents Registration Act, for 6-month period ending February 2026* (Registration No. 5870). US Department of Justice, FARA Registration Unit. https://efile.fara.gov/docs/5870-Supplemental-Statement-20260330-38.pdf

[86]Egan, J., as cited in Meredith, S. (2025, May 13). Why the US is powering Saudi Arabia's AI surge with Nvidia chips. *Fortune*. https://fortune.com/2025/05/13/us-saudi-arabia-trump-ai-nvidia-chips-geopolitical-billions-stake/

[87] Akin Gump FARA Supplemental Statement, Reg. No. 3492, 6-month period ending 12/31/2025, pp. 20, 22–25, 55. https://efile.fara.gov/docs/3492-Supplemental-Statement-20260130-46.pdf

		in the annual National Defense Authorization Act.	securing inclusion in the FY2026 NDAA of Section 1234, which authorizes joint R&D on AI, cybersecurity, quantum computing, and automation at $50 million annually through FY2030. AIPAC spent nearly $1 million lobbying on the NDAA in Q1 2025 alone. Foreign governments frequently pursue NDAA provisions through FARA-registered lobbying firms as a parallel channel.[88]	
B2 — Executive Branch Engagement				
B2.1	**Direct executive agency & rulemaking engagement**	Foreign governments engage US executive agencies through formal comment processes, bilateral co-governance arrangements, or diplomatic-level meetings to shape regulatory frameworks.	**Cybersecurity**: Canada's Communications Security Establishment co-governs the NIST Cryptographic Module Validation Program (CMVP) as a standing bilateral arrangement, directly shaping the cryptographic standards US federal agencies must use in procurement.[89]	*Direct*
B3 — Soft Influence				
B3.1	**Academic & think tank influence**	Foreign governments fund think tanks and support research agendas — shaping the expert knowledge base that informs congressional and agency thinking on technology governance.	**Cybersecurity:** The UAE Embassy and Government of the UK are listed as $1M+ donors in the Atlantic Council's 2024 honor roll; Canada and Japan appear at other contributor levels. The Atlantic Council operates the Cyber Statecraft Initiative, which trains congressional staff on cybersecurity and digital policy through its Congressional Cyber and Digital Policy Program. However, it's noteworthy that this evidence supports access and agenda capacity rather than direct program attribution.[90]	*Direct*
LAYER C — FINANCIAL & ACCESS INSTRUMENTS | Money and relationship-based tools that open doors for Layer B mechanisms to operate effectively				
C1	**Campaign contributions by FARA-registered agents**	Lobbyists acting on behalf of foreign governments make political contributions to US candidates to reinforce access.	No documented example specifically linking foreign government campaign contributions to AI or cybersecurity policy outcomes was identified for the 15-country set. The mechanism is retained based on Freeman & Cleveland-Stout's (2024) finding that	*Direct (amplifier)*

[88] American Israel Public Affairs Committee. (February 1, 2025). *The United States-Israel Defense Partnership Act of 2025* [Bill summary]. https://www.aipac.org/bill-summaries/america-israel-defense-2025; Schwenk, K., & Goldstein, L. (July 23, 2025). AIPAC-backed lawmakers are pushing AI funding for Israel. *Jacobin*. https://jacobin.com/2025/07/aipac-military-ndaa-israel-tech; GovWin IQ. (2025). *Which AI provisions made it into the final FY 2026 NDAA?* Deltek. https://iq.govwin.com/neo/marketAnalysis/view/Which-AI-Provisions-Made-it-into-the-Final-FY-2026-NDAA/8776

[89] National Institute of Standards and Technology. (n.d.). *Cryptographic Module Validation Program*. U.S. Department of Commerce. https://csrc.nist.gov/projects/cryptographic-module-validation-program; Canadian Centre for Cyber Security. (n.d.). *Cryptographic Module Validation Program (CMVP)*. Government of Canada. https://www.cyber.gc.ca/en/tools-services/cryptographic-module-validation-program-cmvp

[90] Atlantic Council. (May 2025). *2024 honor roll of contributors*. https://www.atlanticcouncil.org/in-depth-research-reports/report/2024-annual-report-honor-roll/; Atlantic Council. (n.d.). *Cyber Statecraft Initiative*. https://www.atlanticcouncil.org/programs/cyber-statecraft-initiative/; Atlantic Council. (n.d.). *Congressional Cyber and Digital Policy Program*. https://www.atlanticcouncil.org/programs/cyber-statecraft-initiative/capacity-building-initiative/congressional-cyber-digital-policy-program/

			FARA-registered foreign agents show a strong and consistent correlation between their congressional contacts and their campaign contributions —suggesting that contributions function as access reinforcement for the lobbying activity documented across Layer B mechanisms.[91]	
C2	**Revolving door hiring of former US officials**	FARA-registered lobbying firms hire former US legislators and senior officials, converting their congressional relationships, committee expertise, and institutional knowledge into policy access capacity that amplifies their effectiveness on behalf of foreign principals.	**AI:** Former Rep. Lamar Smith, who chaired the House Science, Space and Technology Committee until January 2019, joined Akin Gump four days after leaving office. By 2022, he had registered as a FARA foreign agent for the UAE Embassy, conducting outreach on export controls, sanctions, and trade policies —issue areas directly relevant to US AI chip export licensing. He was also documented supporting the firm's client work on AI issues, an area directly relevant to his former committee. Former Rep. Ileana Ros-Lehtinen, former Chair of the House Foreign Affairs Committee and member of the House Permanent Select Committee on Intelligence, including its NSA and Cybersecurity Subcommittee, joined the same firm on the same date and, as of January 2026, confirmed in a FARA filing that she serves as Akin Gump Senior Policy Director representing the UAE. Notably, during this period, the firm documented AI cooperation contacts with Senate offices and NEC/EOP staff on behalf of the UAE Embassy.[92]	*Direct (amplifier)*
C3	**Informal diplomatic & social access events**	Foreign government ambassadors and lobbyists arrange informal social events with congressional members and staff, building personal relationships that translate into policy access.	**AI:** In January 2026, former Rep. Ileana Ros-Lehtinen, serving as Akin Gump Senior Policy Director representing the UAE, arranged a US-UAE Business Reception in Miami, bringing together South Florida business leaders with UAE senior diplomats and trade officials from the UAE Embassy —	*Direct (amplifier)*

[91]Freeman, B., & Cleveland-Stout, N. (July 2024). *Foreign lobbying in the U.S.* (Quincy Institute Brief No. 59, p. 24). Quincy Institute for Responsible Statecraft. https://quincyinst.org/research/foreign-lobbying-in-the-u-s/

[92] Joseph, C. & Wright, H. (August 21, 2019). Former Reps. Shuster, Smith, Ros-Lehtinen chaired committees on issues they now lobby on. In *Citizens for Responsibility and Ethics in Washington* (CREW). https://www.citizensforethics.org/reports-investigations/crew-investigations/former-reps-shuster-smith-ros-lehtinen-chaired-committees-on-issues-they-now-lobby-on/; Akin Gump Strauss Hauer & Feld, LLP. (January 7, 2019). *Former Congresswoman Ileana Ros-Lehtinen and Congressman Lamar Smith join Akin Gump* [Press release]. https://www.akingump.com/en/insights/press-releases/former-congresswoman-ileana-ros-lehtinen-and-congressman-lamar; Lamar Smith. (March 31, 2022). *Short form registration statement pursuant to the Foreign Agents Registration Act* (Registration No. 3492). U.S. Department of Justice, FARA Registration Unit. https://efile.fara.gov/docs/3492-Short-Form-20220331-508.pdf; Meyer, T. (January 28, 2020). Ros-Lehtinen registers as a foreign agent. *Politico Influence*. https://www.politico.com/newsletters/politico-influence/2020/01/28/ros-lehtinen-registers-as-a-foreign-agent-784753; Freeman, B., & Cleveland-Stout, N. (August 25, 2022). The spinning door: From US government service to lobbying for dictators. *Responsible Statecraft*. https://responsiblestatecraft.org/2022/08/25/the-revolving-door-from-us-government-service-to-lobbying-for-dictators/; Akin Gump Strauss Hauer & Feld, LLP. (January 13, 2026). *Informational materials filed pursuant to the Foreign Agents Registration Act* (Registration No. 3492). U.S. Department of Justice, FARA Registration Unit. https://efile.fara.gov/docs/3492-Informational-Materials-20260113-281.pdf; Akin Gump Strauss Hauer & Feld, LLP. (January 30, 2026). *Supplemental statement pursuant to the Foreign Agents Registration Act, for 6-month period ending December 2025* (Registration No. 3492, pp. 22–25). U.S. Department of Justice, FARA Registration Unit. https://efile.fara.gov/docs/3492-Supplemental-Statement-20260130-46.pdf

			distributed as FARA informational materials on behalf of the UAE Embassy. Although the event doesn't necessarily mention AI or cyber, it is noteworthy that Akin Gump has been actively representing the UAE on AI-related matters. Additionally, in July 2024, Saudi officials hosted a meeting with a bipartisan congressional staffers' delegation during a regional visit, at which Saudi officials expressed a strong desire to address US concerns about Chinese government activities in Saudi Arabia, specifically in order to receive permission to import US advanced AI chips.[93]	

How to Use This Taxonomy

This taxonomy is designed as a practical analytical instrument. It can be used to:

- Assess which mechanisms are available to a given country based on its institutional assets, Washington access infrastructure, and multilateral positioning.
- Identify where a country's influence efforts are concentrated and where gaps exist.
- Map the governance-influence landscape across a group of countries to identify 69.
- Apply the framework to governance domains beyond cybersecurity and AI — including semiconductors, biotechnology, and quantum computing — that share the same structural features.

Looking Ahead

Two directions build on this taxonomy. First, a companion brief examines the structural differences between cybersecurity and AI safety governance and what they suggest about which mechanisms transfer most readily to AI safety governance now.

Second, applying the taxonomy across the full country set opens the possibility of building country influence types —identifying whether countries cluster into distinct strategies, such as diplomatic multilateralists, security leveragers, or financial actors— and what this suggests for coalition-building in AI safety governance.

Key References

Freeman & Cleveland-Stout (2024), Quincy Institute Brief No. 59 | Keohane & Nye (2011), Power and Interdependence | Cooper (1997), Niche Diplomacy | Büthe & Mattli (2011), The New Global Rulers | Nickerson et al. (2013), EJIS 22(3) | Sangupamba Mwilu et al. (2015), PACIS

[93] Akin Gump Strauss Hauer & Feld, LLP. (January 13, 2026). *Informational materials filed pursuant to the Foreign Agents Registration Act* (Registration No. 3492). U.S. Department of Justice, FARA Registration Unit. https://efile.fara.gov/docs/3492-Informational-Materials-20260113-281.pdf; Alper, A. (July 29, 2024). UAE blocks meetings between AI firm G42 and US congressional staffers, spokesperson says. *U.S. News & World Report*. https://www.usnews.com/news/technology/articles/2024-07-29/uae-blocks-meetings-between-ai-firm-g42-and-us-congressional-staffers-spokesperson-says

POLICY BRIEF 2

Middle Power Levers: What Cybersecurity Governance Teaches AI Safety Policy

Transferable lessons for middle powers seeking to shape US and global AI governance — and where the cyber playbook does not apply

Barbara Marchiori de Assis | SPAR Fellowship | May 2026

Introduction

The two governance domains compared in this brief share structural features that make cybersecurity a legitimate reference case for AI safety governance. Both are **dual-use technologies** whose capabilities can serve civilian or adversarial purposes. Both spread through **a decentralized infrastructure** that no single state can fully control. Both generate **transnational collateral effects** that cross borders in ways difficult to trace or contain. And both are defined by a **pace of technological change** that consistently outstrips institutional capacity to govern it. Because cybersecurity governance has been navigating these features for nearly two decades, it offers a tested set of mechanisms that AI safety governance can study.

That said, the structural differences between the two domains condition which lessons transfer and which do not. Some mechanisms that are well established in cybersecurity are nascent, reconfigured, or simply unavailable in AI. Others have already been activated more forcefully in AI than in cybersecurity, following their own logic. One difference deserves particular attention at the outset: cybersecurity is a *domain organized around a class of digital risks*; AI safety governance is governance of a *technology* whose risks are still being defined. This distinction shapes which actors are relevant. In AI safety, frontier AI labs —a small number of private companies with no close cybersecurity analog— are simultaneously governance participants and targets of influence. Any country seeking to shape AI safety policy must navigate or establish relationships with those actors to a degree that cybersecurity governance does not require.

AI governance is still in the phase of identifying which existing US and global governance pipelines can be repurposed.

Section 1: Two Domains, One Governance Curve

The seven dimensions in the table below are the analytical foundation for the transferability signals developed in Section 2. Understanding *why* the two domains differ across dimensions allows us to identify which mechanisms offer genuine lessons and which require an entirely different framework.

1. Cybersecurity has nearly two decades of multilateral architecture; AI governance has barely two years

Cybersecurity has approximately two decades of accumulated multilateral architecture, while AI has barely two years. The UN General Assembly established the Group of Governmental Experts on ICT security in 2004,[1] and six GGE rounds from 2004 to 2021 produced a normative framework for responsible state behavior, including the application of international law, voluntary peacetime norms, confidence-building measures, and capacity-building commitments.[2] Regional confidence-building measures —16 at the OSCE, 7 at the ASEAN Regional Forum— and the permanent UN mechanism that succeeded the OEWG in 2025 represent a layered institutional ecosystem built over many years. AI governance has no equivalent depth. Although ISO/IEC SC 42 was established in 2017,[3] the first major intergovernmental milestone came only with the Bletchley Declaration (November 2023), followed by the first UNGA resolution on AI (March 2024) and a series of global summits through Seoul (May 2024), Paris (February 2025), and New Delhi (February 2026).[4] The Singapore Consensus on Global AI Safety Research Priorities (May 2025) represents further embryonic steps.[5]

> *For influence purposes, this matters because mature institutions have known access points, established coalitions, and precedents that can be cited. Early-stage institutions are more fluid and more susceptible to first-mover shaping, but offer fewer durable channels.*

2. Cybersecurity has a (somewhat) clear and concentrated regulatory architecture; AI governance authority is fragmented and still forming

In the cybersecurity domain, foreign governments can focus engagement on a small number of identifiable agencies in the US —primarily NIST and CISA— and a layered stack of mandatory instruments: SEC cybersecurity disclosure rules and CIRCIA incident-reporting requirements for critical infrastructure.[6] AI governance does not yet have an equivalent architecture. Multiple US agencies hold partial authority: NIST for risk management frameworks, BIS for chip export controls, OSTP for the executive branch's AI strategy, the FTC for consumer-facing AI products, and sector regulators for domain-specific applications. The relationships between these instruments are still forming.

3. Both domains face private-sector concentration, but the locus differs: vendors and software in cybersecurity, models and compute in AI

In cybersecurity, concentration at the vendor layer —illustrated by the SolarWinds and CrowdStrike incidents— is severe, but the products are, in principle, substitutable. In AI, concentration is more acute and operates at a different layer of the stack. A small number of frontier model providers supply the underlying intelligence for a rapidly expanding set of applications. Unlike cybersecurity software, frontier AI models require training compute and data investments that few actors can replicate, and the companies at the top of the AI stack hold policy leverage with no clear cybersecurity analog.

4. AI infrastructure dependencies create reciprocal leverage that has no counterpart in cybersecurity

Cybersecurity's infrastructure governance drove many countries to invest in local data centers as a sovereignty hedge. AI infrastructure dependencies are structurally harder to replicate: the stack runs from advanced semiconductor fabrication (concentrated at TSMC) through hyperscale cloud compute to foundation model APIs. However, the picture is not one-directional. Major AI companies have actively sought to build data centers in countries with energy surpluses. Gulf states leveraged sovereign wealth and geopolitical ambition to become destinations for global AI infrastructure, with Microsoft committing $15.2 billion to the UAE.[7] In this context, US companies' need to access land, energy, and capital that host countries control creates a reciprocal dependency that gives those countries leverage with no counterpart in classical cybersecurity sovereignty investments.

5. Cybersecurity's national security framing is settled; AI's is shifting rapidly and unevenly across countries

Cybersecurity has long been framed as a national security issue in the US, enabling allied burden-sharing frameworks with clear access rules. Many middle-power countries do not consider AI in the context of national security or great-power competition, and this misalignment of mental models is hindering coalition-building efforts on AI safety. The US government's framing of AI as a strategic competition domain has intensified—but unevenly across countries —creating a coalition-building challenge with no direct cybersecurity parallel.

6. The boundary between AI safety and cybersecurity is blurring, risking fragmented rather than converging governance

Cybersecurity is organized around protection against adversarial actors; AI safety was originally framed around systemic risk posed by the technology itself. This boundary is blurring in both directions. AI models are now deployed as cybersecurity tools; AI systems face adversarial attack vectors of their own. Rather than producing a clean convergence, this could generate fragmentation: cybersecurity forums increasingly absorb AI topics while AI governance forums grapple with security concerns. If the two governance communities do not coordinate, the result may be overlapping but misaligned frameworks. NIST's decision to convene AI and cybersecurity experts through a dedicated effort —producing the Cyber AI Profile (draft December 2025)— underscores the urgency of this coordination challenge.

7. Sovereign investment is constrained in cybersecurity, but is an active policy lever in AI

Cybersecurity's influence is primarily organized around diplomatic engagement, standard-setting, and operational cooperation. Foreign government stakes in US cybersecurity companies face significant CFIUS scrutiny. In AI, the capital requirements for frontier development —model training, data center construction, chip procurement— are large enough to make sovereign wealth fund investment and national compute partnerships into plausible policy levers. Saudi Arabia's Project Transcendence ($100 billion)[9] and the UAE's partnership with MGX in the $100 billion Global AI Infrastructure Investment Partnership (September 2024)[8] illustrate investment flows that create relationships, dependencies, and access operating through commercial rather than diplomatic channels —dynamics the cybersecurity evidence base does not illuminate.

Table 1: How Cybersecurity and AI Safety / Governance Differ as Policy Domains — and Why It Matters for Transferring Influence Mechanisms

What is being compared	Cybersecurity	AI Safety / Governance	Why this difference matters for transferability
1. How long multilateral governance has existed and how developed it is	Approximately two decades of accumulated architecture: six UN GGE rounds (2004–2021), normative framework for responsible state behavior, regional confidence-building measures at the OSCE and ASEAN Regional Forum, and a permanent UN mechanism since 2025–26.	Embryonic: first major intergovernmental milestones only since 2023 (Bletchley Declaration, first UNGA resolution, global summit series through New Delhi 2026, Singapore Consensus).	*Mature institutions have known access points, established coalitions, and precedents that can be cited. Early-stage institutions are more fluid and susceptible to first-mover shaping, but offer fewer durable channels.*
2. How many US agencies govern the domain and whether their instruments are	Few identifiable lead US agencies (NIST, CISA); layered mandatory instruments including SEC cybersecurity disclosure rules and	Authority is fragmented across multiple US agencies (NIST, BIS, OSTP, FTC, sector regulators), with instruments ranging from	*Concentrated regulatory architecture in cybersecurity creates legible engagement*

What is being compared	Cybersecurity	AI Safety / Governance	Why this difference matters for transferability
mandatory or voluntary	CIRCIA incident-reporting requirements for critical infrastructure.	mandatory export controls to voluntary risk management frameworks, and with the relationships between them still forming.	*targets. Fragmented authority and heterogeneous instruments in AI make sustained influence harder to focus and measure.*
3. Where market power is concentrated and whether alternatives exist	Concentration at the vendor and software layer (e.g., SolarWinds, CrowdStrike); substitutable in principle, though switching costs are high.	Concentration at the model and compute layer; few substitutes for frontier models; frontier labs hold disproportionate policy leverage with no close cybersecurity analog.	*In cybersecurity, influence operates largely through government-to-government channels. In AI, middle powers must also navigate a small number of private actors to an extent that has no clear parallel in cybersecurity.*
4. Whether countries can replicate critical infrastructure domestically and what leverage this creates	Many countries built national data centers and local cloud facilities as sovereignty hedges, reducing dependence on US-hosted infrastructure.	AI infrastructure stack (advanced semiconductors, hyperscale compute, foundation model APIs) is harder to replicate domestically, but reciprocal dependency is emerging as AI companies seek land, energy, and capital that host countries control.	*Sovereignty hedges in cybersecurity followed a replicable playbook. AI infrastructure dependencies are structurally different: countries that can offer energy, land, and capital gain leverage that has no direct cybersecurity counterpart.*
5. Whether AI and cybersecurity are treated as national security issues and how consistently across countries	Settled as a national security issue in the US; allied burden-sharing model provides clear access rules for partners.	Not historically framed as a national security issue by most middle powers; framing now shifting rapidly in the US but unevenly across countries, creating misaligned mental models that complicate coalition-building.	*Shared national security framing in cybersecurity enabled allied access and cooperative frameworks. The uneven framing of AI means that influence mechanisms that rely on security partnership logic may not translate straightforwardly.*
6. Whether the boundary between safety and security is clear or blurring	Protection from adversarial actors; clear and settled framing that organizes forum participation and coalition structure.	Originally framed around systemic risk from the technology itself, the boundary is now blurring as AI is deployed as a cybersecurity tool and AI systems face adversarial attack vectors of their own, risking fragmented rather than converging governance.	*Influence built in one forum —cybersecurity or AI— may not carry over into the other, even when both nominally address the same technology, if the two governance communities do not coordinate.*
7. Whether sovereign investment is a viable lever for influencing US policy	Primarily diplomatic and standards-based; foreign government investment in US cybersecurity companies faces significant CFIUS scrutiny,	Large-scale sovereign wealth fund investment, national compute partnerships, and government-backed AI company stakes are active and plausible levers for gaining access and influence in the US AI ecosystem;	*The cybersecurity evidence based on investment as an influence mechanism provides only partial guidance for AI. In AI, commercial and financial channels operate at a scale*

What is being compared	Cybersecurity	AI Safety / Governance	Why this difference matters for transferability
	constraining investment as a direct influence channel.	scale and novelty of these flows have no strong cybersecurity parallel.	*and through structures that the cybersecurity experience does not capture.*

Section 2: What Transfers —and What Doesn't

The following assessment identifies the foreign government influence mechanisms by which the cybersecurity experience provides analytical value to AI safety advocates to shape policy in the US and globally. Only mechanisms with instructive signals are discussed. The assessment is organized first around the mechanisms that transfer most readily, then around those where a different logic applies.

Legend:

★★ **Cyber far ahead**	*Cyber has institutionalized examples; AI has none at a comparable scale* ***(highest-value transferability lesson)***
★ **Cybe ahead**	*Cyber has documented examples; AI has embryonic or no equivalent* ***(important transferability lesson)***
→ **Strong AI-native cases**	*AI has more concrete examples, and sector dynamics benefit AI cases*

TRANSFERS WELL FROM CYBER	ACTIVATED IN AI THROUGH AI-NATIVE DYNAMICS
★★ **A3.1 Multilateral forum leadership** *Procedural consolidation tools; the consolidation phase has not started in AI* ★★ **A3.2 Multilateral institutional redesign** *PoA → Global Mechanism arc; work with the US, not against it* ★ **A3.3 Epistemic framing** *Risk vocabulary for frontier AI is still unsettled and therefore shapeable* ★★ **A4.1 Capacity-building programs** *UK FCDO, Japan AJCCBC, Singapore ASCCE, Canada Global Affairs — pre-shaping third-country positions* ★ **B2.1 Executive agency engagement** *France ANSSI → NIST CSF 2.0 template; Canada CMVP* ★ **B3.2 Think tank & academic funding** *UAE + UK as $1M+ Atlantic Council donors; channel is operational and transferable*	→ **A1.1 Infrastructure investment** *AI is already more active than cyber; AI-native dynamics (sovereign wealth, compute hosting)* → **A2.1 Security alignment leverage** *UAE G42 / Saudi HUMAIN cases*

The multilateral track: where the cyber lessons are richest

A3.1 — Multilateral forum leadership

Both domains have multilateral forum activity; cyber institutional depth is far greater (★★)

The cybersecurity domain has built a multi-layer institutional architecture over fifteen years: UN level (GGE → OEWG → Global Mechanism, 2025),[10] regional level (OSCE 16 CBMs, ASEAN 7 CBMs, OAS/CICTE Working Group, AU Common African Position), operational level (Counter Ransomware Initiative), and capacity-building level (GFCE, AJCCBC, ASCCE). Singapore's deployment of procedural tools during the UN OEWG (2021-25) —the Silence Procedure to bypass vetoes, cumulative framework language to prevent backsliding on prior agreements, and Annual Progress Report drafting to synthesize state interventions— to produce the UN Global Mechanism represents a level of procedural sophistication with no AI analog yet. ISO/IEC SC 27 outputs, meanwhile, were incorporated as informative references in NIST CSF 2.0,[11], illustrating how international standards positions feed directly into US regulatory frameworks.

AI governance has embryonic equivalents: the Singapore Consensus, Bletchley Declaration, ISO/IEC SC 42 (France and India hold convenor positions). However, these are early convening acts, not institutionalized architectures. The cyber experience demonstrates a clear pattern: the most consequential multilateral investments are not the initial forums but the procedural consolidations that come 5–10 years later. AI governance advocates who are investing now in forum creation should plan for the consolidation phase.

A3.2 — Multilateral institutional redesign

Cyber ahead; AI institutional equivalent embryonic (★★)

The cybersecurity case demonstrates that cooperative institutional redesign —proposing a new permanent UN mechanism aligned with the US rather than against it— can succeed. The General Assembly resolution A/RES/77/37, adopted 7 December 2022, was the first UNGA resolution endorsing the Programme of Action (PoA) concept —a proposal for a permanent, inclusive, action-oriented UN mechanism to advance responsible state behavior in cyberspace. France, Japan, and the UK co-sponsored the draft (A/C.1/77/L.73, p.1), and Canada joined as an additional co-sponsor per A/77/380. The PoA process paved the way for the Global Mechanism subsequently established by the OEWG's Final Report (A/80/257) and UNGA-endorsed in December 2025 (A/RES/80/16).[12] The critical lesson is the cooperative framing: middle powers achieved institutional redesign by working with the US. AI governance advocates considering this mechanism should note that the cyber case took three years from the first UNGA resolution to achieve the outcome.

A3.3 — Epistemic framing of risk and governance vocabulary

Cyber ahead; framing embedded in multilateral documents (★)

The UK and France co-launched the Pall Mall Process (2024) to address the proliferation and irresponsible use of commercial cyber intrusion capabilities. The framing —centered on *market governance* rather than outright prohibition— was subsequently adopted in US State Department joint statements on commercial spyware.[13] This is documented epistemic alignment: middle powers helped create a policy category and governance process that US policymakers then used.

The AI safety analog is significant: risk vocabulary for frontier AI —definitions of 'frontier model', 'catastrophic risk', 'safety evaluation', 'responsible scaling'— is still unsettled and therefore actively shapeable. Middle powers that engage now in defining these terms within ISO/IEC SC 42, GPAI, and the AI safety summit process occupy the same epistemic position that the UK/France held at the start of the Pall Mall Process.

A4.1 — Capacity-building and institutional diffusion Cyber far ahead; highest-value transferability lesson (★★)

Capacity-building is identified across the assembled evidence as one of the six most consistently powerful middle-power influence channels in the cybersecurity domain. Four documented programs illustrate the mechanism:

- UK FCO/FCDO (2016–2021, with further expansion thereafter): A cyber capacity-building programme explicitly framed around 'transformational projects aligned with clear UK interests' — funding projects across Eastern Europe, ASEAN, MENA, India, Brazil, and Mexico — illustrating that the UK treats capacity-building as an instrument of national security and foreign policy alongside partner development.[14]
- Japan AJCCBC (Bangkok, 2018–present): The ASEAN–Japan Cybersecurity Capacity Building Centre, established in 2018 with Japanese government funding, trains government officials and critical information infrastructure operators from all 10 ASEAN member states in cyber defense, forensics, and malware analysis. Phase One ran through 2022; Phase Two (2023–2027), implemented by JICA and Thailand's National Cyber Security Agency, continues the programme under an expanded mandate covering trusted digital services. Murphy & Nagy (2024) identify Japan's material drivers as prestige as a regional leader, politico-diplomatic concerns, and promoting economic development by creating advanced markets.[15]
- Singapore ASCCE (2019–2024): The ASEAN–Singapore Cybersecurity Centre of Excellence, funded by Singapore with a five-year, SGD $30 million commitment, trained over 900 senior government officials from ASEAN and beyond across more than 30 programmes, covering international law, cyber strategy, legislation, and cyber norms —pre-shaping the positions ASEAN members bring to multilateral forums where the US is present. The ASCCE collaborated with partners including Australia, Canada, Japan, the UK, and the United States.
- Canada Global Affairs (2015–present): Since 2015, Global Affairs Canada has contributed over $13 million to cyber capacity-building projects worldwide, helping 10 countries in the Americas develop national cyber strategies and supporting the development or improvement of 17 Computer Security Incident Response Teams throughout the Americas —explicitly framed by the Canadian government as building a common understanding of responsible state behaviour in cyberspace in line with the 2015 GGE norms[16]

AI safety has embryonic equivalents: the UK's AI Safety Institute and the Bletchley framework are beginning to extend into AI governance capacity-building for third countries.

B2.1 — Executive agency and rulemaking engagement

Cyber ahead; CMVP co-governance model (★)

The NIST AI Risk Management Framework (January 2023) is structurally identical to NIST CSF 2.0 as a foreign government influence venue: public comment process, voluntary compliance structure, informative references to international standards. France's ANSSI submitted comments on the NIST CSF 2.0 public draft, explicitly mapping EU NIS II pillars to CSF 2.0 functions and proposing that NIST flag this alignment as a way to 'bridge US and European approaches.[17] This precedent is directly transferable to NIST AI RMF engagement —the channel is open, has precedent for foreign government participation, and no documented foreign government submission to the NIST AI RMF process has yet been identified.

An interesting case is Canada’s CMVP model: a standing bilateral arrangement in which Canada’s Communications Security Establishment co-governs NIST’s Cryptographic Module Validation Program, directly influencing the cryptographic standards US federal agencies must use in procurement.[18] An AI equivalent might take the form of a joint foreign-government / NIST AI evaluation framework.

One important structural complication: the multiplicity of AI agency jurisdictions (NIST, OSTP, BIS, FDA, FTC, sector regulators) makes B2.1 more complex than in cybersecurity. Influence on NIST AI RMF does not automatically translate to influence on BIS export control policy or OSTP directives.

B3.2 — Academic and think tank funding

Cyber ahead; channel operational and directly transferable (★)

Foreign government funding of US think tanks with relevant policy programs is directly documented. The Atlantic Council —which operates the Cyber Statecraft Initiative, training congressional staff on cybersecurity and digital policy through its Congressional Cyber and Digital Policy Program— lists the UAE Embassy and the Government of the UK among its $1 million-or-above donors in its 2024 annual honor roll.[19] Canada and Japan appear at other contributor levels. This evidence supports access and agenda-setting capacity; it does not constitute direct program attribution, though.

The AI safety analog is available and requires minimal adaptation: major US think tanks and university AI governance programs are direct equivalents to the Cyber Statecraft Initiative. In AI, an additional observation applies: frontier labs are also influenced targets alongside government actors, meaning that think tanks and academic networks that bridge between government and lab communities carry particular value.

Where the cyber playbook may not apply

> **A1.1 — Infrastructure investment & strategic hosting | A2.1 — Security alignment leverage**
>
> Strong AI-native cases (→)

Infrastructure investment (A1.1) and security alignment leverage (A2.1) are already very active in AI. The UAE's G42–Microsoft deal, Stargate UAE, and Microsoft's $15.2 billion UAE investment are AI-domain-native activations of A1.1 with no cybersecurity counterpart. The UAE G42 and Saudi HUMAIN security-for-chips exchanges (A2.1) represent bilateral leverage dynamics mediated through discrete, licensable hardware —making credible commitment and verification tractable in a way that cybersecurity cooperation, which is more diffuse and relationship-based, does not replicate.

Note on trade-embedded provisions (A1.2)

Canada and Mexico's cybersecurity cooperation provisions in USMCA Article 19.15 (2020) —subsequently copied nearly word-for-word in the US–Japan Digital Trade Agreement— provide a documented template for embedding technology governance cooperation clauses in trade instruments.

Section 3: Three Priorities for AI Safety Advocates

THREE PRIORITIES FOR AI SAFETY ADVOCATES

01

Build multilateral procedural capacity now

A3.1 · A3.2 · A3.3

The cyber experience shows that multilateral governance typically begins through convening mechanisms and procedural engagement within existing

02

Invest in capacity-building in third countries

A4.1

Cybersecurity's most consistently powerful middle-power channel —documented across the UK FCDO, Japan's AJCCBC, Singapore's ASCCE,

03

Engage US regulatory processes directly

B2.1

The NIST AI Risk Management Framework (January 2023) was developed through the same public comment process as NIST CSF 2.0 —a

forums before reaching more institutionalized forms. The GGE/OEWG processes illustrate this: sustained procedural participation over multiple rounds created the normative consolidation and coalition infrastructure that eventually made a permanent mechanism viable.	and Canada's Global Affairs programming— is the pre-shaping of third-country positions before those countries enter multilateral forums where the US is also present.	process that is structurally open to foreign government participation. The cybersecurity experience shows that middle-power regulatory agencies have engaged this channel directly: formal submissions to NIST rulemaking processes are a documented mechanism for shaping how US standards frameworks are written.

Looking Ahead

This brief is the second in a series. The third builds on the taxonomy to develop **country profiles** for each of the 15 countries in the study set, mapping which levers each country is currently deploying across Layers A, B, and C —and identifying how each country could position itself more strategically in AI safety governance given its institutional assets, Washington access infrastructure, and multilateral positioning.

The analytical framework, full evidence base, and country-level assessments for this brief are documented in the companion working paper: Marchiori de Assis, B. (forthcoming, July 2026). 'Middle Power Levers: Lessons from Cybersecurity for AI Safety Governance.' SPAR Fellowship Research Paper.

Endnotes

1. DW Observatory. "UN Global Mechanism on Cybersecurity." https://dig.watch/processes/un-gge — section "Past processes: the GGEs and OEWGs "In 2004, the UN General Assembly established the Group of Governmental Experts to examine the impact of developments in ICT on national security and military affairs."

2. The Hague Center for Strategic Studies (December 2021). "The Evolution of the UN Group of Governmental Experts on Cyber Issues." https://hcss.nl/wp-content/uploads/2021/12/Klaar.pdf — pp. 1–3, discussion of the four-element normative framework produced across six GGE rounds.

3. ISO/IEC JTC 1/SC 42. (November 2024). ISO/IEC JTC 1/SC 42 Artificial Intelligence. Retrieved from https://jtc1info.org/sd-2-history/jtc1-subcommittees/sc-42/

4. UK (November 2023). The Bletchley Declaration by Countries Attending the AI Safety Summit, 1-2 November 2023. Retrieved from https://www.gov.uk/government/publications/ai-safety-summit-2023-the-bletchley-declaration/the-bletchley-declaration-by-countries-attending-the-ai-safety-summit-1-2-november-2023; United Nations General Assembly. (March 2024). Seizing the opportunities of safe, secure and trustworthy artificial intelligence systems for sustainable development (Resolution A/RES/78/265). United Nations. Retrieved from https://digitallibrary.un.org/record/4043244. Future of Life Institute. (n.d.). AI safety summits. Retrieved from https://futureoflife.org/project/ai-safety-summits/; India (February 2026). India AI Impact Summit 2026. Retrieved from https://impact.indiaai.gov.in/

5. Singapore Infocomm Media Development Authority. (May 2025). The Singapore Consensus on Global AI Safety Research Priorities: Building a Trustworthy, Reliable and Secure AI Ecosystem. Retrieved from https://file.go.gov.sg/sg-consensus-ai-safety.pdf

6. NIST (February 2024). "The NIST Cybersecurity Framework (CSF) 2.0". Retrieved from https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf; SEC (July 2023). "SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies." Retrieved from https://www.sec.gov/newsroom/press-releases/2023-139; Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA). Retrieved from https://www.congress.gov/bill/117th-congress/house-bill/2471; https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia. NIST (January 2023). "Artificial Intelligence Risk Management Framework (AI RMF 1.0)." Retrieved from https://www.nist.gov/itl/ai-risk-management-framework

7. PWC (April 2025). “Unlocking the data center opportunity in the Middle East.” Retrieved from https://www.pwc.com/m1/en/media-centre/articles/unlocking-the-data-centre-opportunity-in-the-middle-east.html; Microsoft (November 2025). “Microsoft’s $15.2 billion USD investment in the UAE.” Retrieved from https://blogs.microsoft.com/on-the-issues/2025/11/03/microsofts-15-2-billion-usd-investment-in-the-uae/.

8. Crowell & Moring (September 2025). "The Middle East's Big Bet on Artificial Intelligence and Data Security." https://www.crowell.com/en/insights/client-alerts/the-middle-easts-big-bet-on-artificial-intelligence-and-data-security — paragraph: "In September 2024, BlackRock, Global Infrastructure Partners, Microsoft, and MGX inaugurated a new AI partnership to invest in data centers and power infrastructure with a potential for $100 billion investment in the United States and abroad."

9. Digital Bricks (July 2025). "The State of AI in the Middle East (2025)." https://www.digitalbricks.ai/blog-posts/the-state-of-ai-in-the-middle-east-2025 — paragraph: "Saudi Arabia likewise views AI as essential to its Vision 2030 economic transformation plan… In late 2024, Saudi Arabia announced 'Project Transcendence,' a $100 billion AI initiative aimed at turning the country into a global AI powerhouse."

10. UN General Assembly (July 2025). Final report of the open-ended working group on security of and in the use of information and communications technologies 2021-2025. Retrieved from https://docs.un.org/en/A/80/257; United Nations General Assembly. (December 2025). Developments in the field of information and telecommunications in the context of international security (Resolution A/RES/80/16). New York: United Nations. Retrieved from https://docs.un.org/en/A/RES/80/16; DigWatch, UN global mechanism on cybersecurity. Retrieved from https://dig.watch/processes/un-gge; Rupp, C. (March 2026). “The UN’s New Global Mechanism on Cybersecurity: How Europe Can Advance Responsible State Behavior in Cyberspace.” In Interface. Retrieved from https://www.interface-eu.org/publications/the-new-united-nations-mechanism-on-cybersecurity

11. ISO. (n.d.). ISO/IEC JTC 1/SC 27 participation register. https://www.iso.org/committee/45306.html?view=participation; NIST. (n.d.). CSF 2.0 Informative References. https://www.nist.gov/cyberframework/informative-references

12. UN Office for Disarmament Affairs – UNODA (2021). Working Paper for a Programme of Action (PoA) to advance responsible state behavior in the use of ICTs in the context of international security. Retrieved from https://documents.unoda.org/wp-content/uploads/2021/11/Working-paper-on-the-proposal-for-a-Cyber-PoA.pdf; UN General Assembly (7 December 2022), A/RES/77/37, “Programme of action to advance responsible State behavior in the use of information and communications technologies in the context of international security”. Retrieved from https://digitallibrary.un.org/record/3997617?ln=en; UN General Assembly (24 October 2002), A/C.1/77/PV.19, Retrieved from https://docs.un.org/en/A/C.1/77/PV.19; UN General Assembly. (14 November 2022). Developments in the field of information and telecommunications in the context of international security: report of the 1st Committee: General Assembly, 77th session. Retrieved from https://digitallibrary.un.org/record/3995343?v=pdf; UN General Assembly. (10 November 2023). Report of the First Committee: Developments in the field of information and telecommunications in the context of international security (A/78/404). Retrieved from https://undocs.org/A/78/404; UN General Assembly. (4 December 2023). Programme of action to advance responsible State behavior in the use of information and communications technologies in the context of international security (A/RES/78/16). https://undocs.org/A/RES/78/16; UN General Assembly (July 2025). Final report of the open-ended working group on security of and in the use of information and communications technologies 2021-2025. Retrieved from https://docs.un.org/en/A/80/257; United Nations General Assembly. (December 2025). Developments in the field of information and telecommunications in the context of international security (Resolution A/RES/80/16). New York: United Nations. Retrieved from https://docs.un.org/en/A/RES/80/16; DigWatch, UN global mechanism on cybersecurity. Retrieved from https://dig.watch/processes/un-gge; Rupp, C. (March 2026). “The UN’s New Global Mechanism on Cybersecurity: How Europe Can Advance Responsible State Behavior in Cyberspace.” In Interface. Retrieved from https://www.interface-eu.org/publications/the-new-united-nations-mechanism-on-cybersecurity; Delegation of the EU to the UN in New York (September 2025). UN Member States agree to establish a global mechanism to advance responsible state behavior in cyberspace. Retrieved from https://www.eeas.europa.eu/delegations/un-new-york/un-member-states-agree-establish-global-mechanism-advance-responsible-state-behaviour-cyberspace_en; Pytlak, A. (August 2025). “Cyber Diplomacy 2.0: From Process to Impact.” In Stimson. Retrieved from https://www.stimson.org/2025/cyber-diplomacy-2-0-from-process-to-impact/; Pavlova, P. & Painter, C. (August 2025). “The UN’s Permanent Process on Cybersecurity Faces an Uphill Battle.” In Lawfare. Retrieved from https://www.lawfaremedia.org/article/the-un-s-permanent-process-on-cybersecurity-faces-an-uphill-battle.

13. Foreign, Commonwealth, & Development Office – FCDO (February 2024). The Pall Mall Process: tackling the proliferation and irresponsible use of commercial cyber intrusion capabilities. Retrieved from https://www.gov.uk/government/publications/the-pall-mall-process-declaration-tackling-proliferation-and-irresponsible-use-of-commercial-cyber-intrusion-capabilities/the-pall-mall-process-tackling-the-proliferation-and-irresponsible-use-of-commercial-cyber-intrusion-capabilities; US Department of State (September 2024). Joint Statement on Efforts to Counter the Proliferation and Misuse of Commercial Spyware. Retrieved from https://2021-2025.state.gov/office-of-the-spokesperson/releases/2024/09/joint-statement-on-efforts-to-counter-the-proliferation-and-misuse-of-commercial-spyware; US Mission to International Organizations in Geneva (October 2024). US Advances UN Recognition of Threats Posed by Commercial Spyware. Retrieved from https://geneva.usmission.gov/2024/10/11/u-s-advances-un-recognition-of-threats-posed-by-commercial-spyware/; France Diplomacy (April 2025). Pall Mall Process: Code of Practice for States to tackle the proliferation and irresponsible use of commercial cyber intrusion capabilities. Retrieved from https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/news/article/pall-mall-process-code-of-practice-for-states-to-tackle-the-proliferation-and?page_courante=1#pagination_ssra; FCDO (October 2025). The Pall Mall Process Code of Practice for States. Retrieved from https://www.gov.uk/government/publications/the-pall-mall-process-code-of-practice-for-states/the-pall-mall-process-code-of-practice-for

-states; FCDO (January 2026). UK and France seek views on commercial cyber intrusion industry practices. Retrieved from https://www.gov.uk/government/news/uk-and-france-seek-views-on-commercial-cyber-intrusion-industry-practices

14. FCO Cyber Security Capacity Building Programme (16 November 2016). GOV.UK. https://www.gov.uk/government/news/fco-cyber-security-capacity-building-programme; FCO Cyber Security Capacity Building Programme 2018 to 2021 (15 January 2018). GOV.UK. https://www.gov.uk/government/publications/fco-cyber-security-capacity-building-programme-2018-to-2021; European Union Institute for Security Studies (2021), International Cyber Capacity Building: Global Trends and Scenarios, Annex 3, p. 3, https://www.iss.europa.eu/sites/default/files/EUISSFiles/CCB%20Annex%203%20Final_0.pdf (documenting the programme's expansion and evolution through 2021).

15. Cybil Portal (January 22, 2025), ASEAN–Japan Cybersecurity Capacity Building Centre (AJCCBC) – Phase One, https://cybilportal.org/projects/asean-japan-cybersecurity-capacity-building-centre/; Cybil Portal, AJCCBC Phase Two, https://cybilportal.org/projects/project-for-enhancing-asean-japan-capacity-building-program-for-cybersecurity-and-trusted-digital-services/; Murphy, T. & Nagy, S. (2024). Middle-power cybersecurity in the Indo-Pacific. Journal of Intelligence, Conflict, and Warfare, 7(1), 1–24.

16. Cybil Portal, ASEAN–Singapore Cybersecurity Centre for Excellence (ASCCE), https://cybilportal.org/projects/asean-singapore-cybersecurity-centre-for-excellence-ascce/ (status: finished, September 2019–September 2024); Cyber Security Agency of Singapore (CSA), ASEAN-Singapore Cybersecurity Centre of Excellence, https://www.csa.gov.sg/news-events/press-releases/asean-singapore-cybersecurity-centre-of-excellence/; Global Affairs Canada (last modified December 20, 2023). International cyber policy — Capacity building. https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/cyber_policy-politique_cyberspace.aspx?lang=eng

17. ANSSI (21 August 2023). Comments on NIST CSF 2.0 (public draft), submitted to NIST. US Department of Commerce / NIST. https://www.nist.gov/document/08212023-anssi-np-comments-nist-csf-20 (rows 1–2, global comments)

18. National Institute of Standards and Technology. (n.d.). Cryptographic Module Validation Program. U.S. Department of Commerce. https://csrc.nist.gov/projects/cryptographic-module-validation-program; Canadian Centre for Cyber Security. (n.d.). Cryptographic Module Validation Program (CMVP). Government of Canada. https://www.cyber.gc.ca/en/tools-services/cryptographic-module-validation-program-cmvp

19. UAE Embassy and UK Government as $1M+ Atlantic Council donors: Atlantic Council (May 2025), 2024 Honor Roll of Contributors, https://www.atlanticcouncil.org/in-depth-research-reports/report/2024-annual-report-honor-roll/; Atlantic Council (n.d.), Cyber Statecraft Initiative, https://www.atlanticcouncil.org/programs/cyber-statecraft-initiative/; Congressional Cyber and Digital Policy Program, https://www.atlanticcouncil.org/programs/cyber-statecraft-initiative/capacity-building-initiative/congressional-cyber-digital-policy-program/

Can Middle Powers Decelerate Frontier AI Race Dynamics?

Caleb Peppiatt[94]

Executive Summary

Competitive race dynamics between the United States and China constrain both superpowers' ability to unilaterally decelerate frontier AI development. However, coalitions of middle powers may help decelerate racing through supporting *multi-track diplomacy*, *norm entrepreneurship*, and *conflict mediation*. The effectiveness of such mechanisms depends upon the proactive agency of middle powers in agenda-setting in international fora, their degree of normative unity, and the willingness of the United States and China to engage in international AI governance initiatives. These factors are evaluated through the thematic coding of six middle powers' policy documents, finding that there is a moderate degree of political will to contribute to pro-safety international governance.

Introduction

The United States of America and the People's Republic of China are widely believed to be "racing" in frontier AI development. This is typically framed either in terms of i) a race to develop a mature national system of innovation, integrating AI into their domestic economy, and leading in global AI markets (Schmid et al: 2025; Wang and Siler-Evans: 2026; Sytsma: 2026); ii) a set of races to develop military-AI applications, such as in cyber, electronic, and autonomous warfare (Eslami et al: 2025); and iii) a race to develop especially powerful, generally-capable models - "AGI" or "ASI" (Dung and Hellrigel-Holderbaum: 2025). This report shall consider each of these framings - *economic*, *military*, and *AGI*, specifying which mechanisms are particularly relevant for each framing.

[94] Science Policy Research Unit (SPRU), University of Sussex. Special thanks to SPRU colleagues Pavel Casian and Athar Mubarak for help in thematic coding, and SPAR colleagues Aris Richardson and Adam Hassan for help with initial framing.

Such superpower racing is geopolitically destabilising (Cave and ÓhÉigeartaigh: 2018). Military procurement is accelerating, increasing the risks of irresponsible technological development and deployment (Schwarz: 2025). Racing to develop highly capable models so as to achieve unilateral dominance comes with multiple, independent catastrophic risks, including loss of control over misaligned AGI, preventive wars, and system misuse (Dung and Hellrigel-Holderbaum: 2025). Aside from exacerbating the odds of great power conflict, racing towards developing superintelligence may plausibly result in the extreme concentration of power, undermining democratic institutions (Katzke and Futerman: 2024). Such racing is not inevitable, and superpower behaviour may be influenced by internal pressures, the behaviour of other states, and the broader geopolitical environment.

Recent research has explored the potential roles of middle powers in influencing race dynamics. Middle powers may seek to carve out niches in semiconductor supply chains to gain leverage over race outcomes, align themselves fully with a superpower - supplying research talent, hosting data centres, and co-developing military-AI systems - or else hedge and become entangled in both American and Chinese AI ecosystems (Sandoval and Wilkinson: 2026, Tran: 2026). More optimistically, middle powers may instead seek to *decelerate* both superpowers' frontier AI development, either out of pragmatic self-interest or due to internalised pro-safety norms. Potential mechanisms here include multi-track diplomacy to establish a shared scientific consensus over risks from capable AI systems (Flink and Schreiterer: 2010), agenda-setting in international fora so as to coordinate the joint development of standards (Fort: 2024), the entrepreneurship and diffusion of pro-safety norms (Allen and Liao: 2025), and brokering dialogues to facilitate conflict mediation (Valeriani and Polito: 2025). Perhaps most ambitiously, it has been proposed that a coalition of middle powers might impose comprehensive export controls and pre-emptive targeting against states pursuing the development of superintelligence (Amadori *et al:* 2025).

Each of these purported mechanisms were initially stress-tested through exploratory scenario mapping (Pavel et al: 2025), in order to identify salient factors affecting their plausibility. Middle power deceleration mechanisms depend on several variables: the degree of normative unity between middle powers - how aligned middle powers are in their AI governance priorities, norms, and coordinated efforts; the degree of political will held by middle powers in pursuit of deceleration (the reputational, regulatory, and geopolitical costs that middle powers are willing to accept to decelerate AI racing); and the

willingness of the U.S.A. and the P.R.C. to engage in international governance initiatives. The rest of this report shall explain the methodology by which these variables were evaluated, present and discuss findings for a set of prominent middle powers, and outline directions for future research on concrete "windows of opportunity" in which middle power-mediated deceleration might occur.

Theory and Methodology

The effectiveness of scenarios involving multi-track diplomacy, agenda-setting for standardisation, norm entrepreneurship and diffusion, and dialogue brokerage in part depends upon the *normative unity* and *political will* of middle powers.

To illustrate the importance of *normative unity*, several analysts have proposed that the deceleration of harmful AI race dynamics may be aided by the International Network of AI Safety Institutes (AISIs). The U.K. pioneered the establishment of an AI Safety Institute in 2023, effectively promoting awareness of catastrophic risks from AI internationally through the Bletchley Park AI Safety Summit. The Network may help decelerate race dynamics by building an international consensus around risks from advanced AI systems (Allen and Adamson: 2024; for an example of multilateral consensus-building, see Bengio *et al:* 2024), and by hosting technical working groups to establish interoperable model evaluation frameworks and standards (Cihon: 2019). China's equivalent institution to Western AISIs was established in February 2025, and openly calls for greater cooperation in standards development and safety policy (Singer, Elmgren and Guest: 2025). The Network might engage in sustained standardisation efforts with the China AI Safety and Development Association, thereby building mutual trust between the U.S. and China and forwarding technical harmonisation initiatives (Fort: 2024, 9). The current Network would have to expand or adapt to incorporate Chinese stakeholders to a greater degree (Velasco *et al:* 2025; Ryan, Iliadis, and Gor: 2024, 13-18). Such institutional reform requires sustained political will from middle powers within the Network, as well as a willingness to broaden the Network's substantive participation to include non-U.S.-aligned actors. It would also require substantial normative unity between middle power

members: if several members were unwilling to pursue pro-safety policies, or adopted a highly securitised, antagonistic stance towards Chinese participation, then technical harmonisation efforts are unlikely to succeed. In each of these cases, the feasibility of proposed coalitions between middle powers depends in part on the degree of *normative unity* between members: if Singapore uses the Network to promote the expansion of an open and interoperable digital market (Allen and Liao: 2025), whereas the U.K. and France pursue proprietary "innovation-first" agendas, or if Canada favours brokering U.S.-China dialogues, whereas Japan is wary of security implications, coalitions could fragment.

Other proposed fora for international AI governance may be less dependent on the degree of normative unity between middle powers, yet still requires sustained *political will* on behalf of a smaller group of actors. A strong example of middle power agency lies in the hosting of annual AI Safety Summits: The U.K. and South Korea both established significant pro-safety agendas for discussion, working groups, and summit declarations in 2023 and 2024 (Buhl, Bucknall and Masterson: 2025); France essentially shifted the purpose of the summits to become business-showcase events in 2025, a move emulated by India in 2026. As such, individual middle powers may exercise oversized influence by hosting and setting the agenda for future summits. Switzerland shall host the 2027 summit alongside the United Nations International Telecommunications Union (DETEC: 2025), offering a lucrative opportunity for standard-setting, while the U.A.E. shall host the 2028 summit.[95] If these summits are to produce concrete policies or international commitments, the middle power hosts must exercise sustained political will, which includes non-hostile attitudes towards both superpowers. For a summit to successfully broker U.S.-China dialogues, preparatory events should be held - such as the July 2026 "AI for Good Global Summit" hosted by the ITU and Swiss Government, sufficient time should be allocated for technical working groups for the establishment of shared standards, and the normative priorities of the summit ought to be clear in advance. In contrast, a summit is unlikely to offer a venue for substantive dialogues and technical harmonisation if the host country lacks the political will to serve as a neutral third-party. The middle power host must instead be willing to bear economic and geopolitical costs in setting a pro-safety agenda - such as the opportunity cost of using the summit to attract foreign AI firms, or the risk of alienating one superpower by attempting to promote international coordination.

[95] The Swiss Federal Department of Foreign Affairs and the International Telecommunications Union have stated in personal correspondence that they are still preparing the agenda and priorities for the 2027 summit, and so are unable to confirm their stated aims for the event.

In order to evaluate the degree to which middle powers are normatively unified and politically willing to decelerate frontier AI race dynamics, qualitative thematic analysis was employed. Five-hundred excerpts from over ninety documents (diplomatic statements, national AI strategies, and government reports) were analysed according to an *a priori* coding framework. Six countries' national priorities, attitudes towards Chinese involvement in AI governance, attitudes towards binding international commitments on AI safety, and preferences concerning the evaluation of AI systems were systematically recorded using Dedoose. Middle powers were selected based on their roles as hosts of annual AI safety summits, or their roles as norm entrepreneurs in past multilateral governance efforts. Thematic analysis provides more detailed overviews of countries' political stances and norms than documenting declarations which the country has signed (fig. 1). While publicly-accessible government documents may include noise that diverges from a country's genuine policy preferences, triangulating sources from different departments, contexts, and modalities (such as comparing ministerial statements to stated military policy) offers a nuanced understanding of a nation's priorities in international AI governance. Finally, to ensure the reliability of thematic coding, analyses were checked by two independent colleagues.

(Fig. 1: AI Middle Powers as Signatories. Due to reputational incentives, signing a declaration alone does not offer sufficient insight into normative unity and political will).

Document	United Kingdom	Singapore	Japan	France	UAE	Switzerland
AI Safety Summit 2023 Declaration	Signed	Signed	Signed	Signed	Signed	Signed
AI Summit 2024 Declaration	Signed	Signed	Signed	Signed	Not included	Not included
AI Summit 2024 Ministerial Statement	Signed	Signed	Signed	Signed	Signed	Signed
AI Action Summit 2025 Statement on Inclusive and Sustainable AI	Not signed	Signed	Signed	Signed	Signed	Signed
AI Impact Summit 2026 Declaration	Signed	Signed	Signed	Signed	Signed	Signed
Responsible AI in Military Domain Summit 2023 Call to Action	Signed	Signed	Signed	Signed	Not signed	Signed
Responsible AI in Military Domain Summit 2024 Blueprint for Action	Signed	Signed	Signed	Signed	Unknown	Signed
Responsible AI in Military Domain Summit 2026 Pathway to Action	Signed	Signed	Signed	Signed	Not signed	Signed

Results

Japan's national priority is economic competitiveness, in line with Society 5.0 initiatives (AI Strategy 2022, "Promotion of AI" Act 2025, AI Strategic Council 2025). Central government policies aim to

accelerate technology adoption, to promote business overseas, and to reinforce national strengths in health, agriculture, and transportation sectors. An adversarial attitude towards China is evident in the security literature (US-Japan Joint Security Statement 2024, the Japan Economic Security Act 2022, the National Defense Strategy 2022, and the Japan-US Technology Agreement 2025). Despite this, Japan views itself as a leader in the international coordination of AI governance efforts, and as a promoter of international norms. This includes the promotion of standardisation activities and participation in the AISI Network, with J-AISI established in 2024. The 2023 Hiroshima Process generally aligns with the OECD AI Principles that Japan helped promote, yet predominantly places the regulatory burden onto developers, rather than partnered states. It has expanded through the Hiroshima AI Process Friends Group to 50 countries since 2024. Domestically, Japan seeks to minimise regulatory burdens, favouring agile governance and "pluralistic interoperability." Its national strategy favours soft laws and sector-specific guidelines, rather than *ex ante* risk-based legislation.

France's national priority is also economic competitiveness, framed primarily in terms of increased private investment, the development of national champions, and the pursuit of "technological sovereignty" (2021 National AI Strategy, 2025 AI Commission Report). Their AI Action Summit of 2025 attempted to present an optimistic, business-friendly environment, such that AI safety was diminished in favour of business opportunities by director Anne Bouverot. The Summit's concluding declaration on Inclusive and Sustainable AI was accepted by China, but not the United Kingdom. Unlike Japan, France has secured a strong relationship with China with regards to AI governance (2024 Joint French-Chinese Statement on AI). The 2025 Commission Report argues that, 'in the current context of heightened economic competition between the United States and China, France could appear as a point of equilibrium, favouring the rapid emergence of a form of governance that includes elements of regulation, standardisation and auditing.' Through INESIA, France signals active participation in the Network of AISIs. More concretely, the INESIA roadmap for 2026-7 supports the establishment of a modular platform that enables the reproducible and interoperable evaluation of AI models. Domestically, France favours interoperable data governance legislation, aiming to synthesise both pro-innovation and pro-safety stances through the EU AI Act.

The United Kingdom's national priority is supporting an innovative AI ecosystem at home (2021 National AI Strategy, 2025 AI Opportunities Plan). At the same time, the U.K. hosted the inaugural AI Safety

Summit, promoted catastrophic risk concerns through the 2023 Bletchley Declaration, and has advocated greater cooperation over shared model evaluation tools and interoperable governance frameworks (Ministerial Statement, 2024). While Sunak's government invited China to the 2023 AI Safety Summit, the content of the recent 10th Strategic Dialogue with China was strategically vague. 2025 saw heightened security concerns and greater alignment with the Trump Administration's priorities: The AISI was renamed from a "Safety Institute" to a "Security Institute," and the 2025 AI Action Plan suggests building computational infrastructure only with "likeminded countries." There is strong participation in voluntary domestic and international governance schemes, such as the Hiroshima Process International Code of Conduct for Advanced AI Systems, the OECD AI Principles, and a non-binding memorandum of understanding with OpenAI, yet aligned with the U.S. against signing the French AI Action Summit declaration of 2025, referring to a lack of detail over the proposed AI governance mechanisms.

Singapore's national priority is the adoption of AI in sectors so as to improve public services delivery and to secure economic gains (the 2023 National AI Strategy 2.0). Singapore has extensively advocated the interoperability of digital markets and norms of international collaboration (2026 Model AI Governance Framework, AI Verify, 2025 Singapore Consensus on Global AI Safety Research Priorities). Singapore has been diplomatically active on both regional and international bases, coordinating economically through the ASEAN Working Group on AI Governance (WG-AI), and hosting REAIM Summits on Military AI. Singapore constitutes a major market in both U.S. and Chinese AI ecosystems, and a bilateral data-sharing agreement with China on civilian applications of AI in 2025 encouraged 'all countries to set aside the instinct of protectionism, to steer AI as a force for good.' Singapore fosters AI Verify as an international open-source community for AI testing tools, to 'create a neutral platform for open collaborations and idea-sharing.' It has consistently advocated interoperability in digital markets, a priority which aligns with both economic self-interest and the deceleration of zero-sum race dynamics (Allen and Liao: 2025; Cheng, Chong and Gomez: 2026; Chin *et al:* 2026).

Switzerland's national priority is also economic competitiveness - seeking to maintain its reputation as a business hub - within the bounds of respect for fundamental human rights, democracy, and the rule of law (2024 Council of Europe's Framework Convention on AI). Switzerland prioritises its reputation for neutrality, high institutional trust, and prior embeddedness in international diplomacy. They tend to employ a rights-based, sector-specific governance model, with central themes including data protection,

redress, and transparency (E.U. AI Act). The country is hosting the 2027 summit alongside the ITU, and both are laying the groundwork for the summit through the UN's inaugural Global Dialogue on AI Governance and AI for Good's Open Dialogue on Trustworthy AI in July 2026.

The *United Arab Emirates'* normative priorities and political will in hosting the 2028 summit are somewhat opaque: national strategies suggest that AI is viewed as a resource for leadership in the Gulf, for the digital transformation of government services, and for economic diversification (Kalviri: 2025; Albous *et al:* 2025, p. 2406). While the U.A.E. references "responsible AI governance" consistently in public discourse, this concept is framed instrumentally in support of facilitating trusted investments, and domestic governance relies on voluntary risk management procedures and sectoral guidelines.

Discussion

The six middle powers analysed display divergent national priorities and varying degrees of political will. Optimistically, several middle powers perceive themselves as facilitators of international AI governance, AI safety policy, and U.S.-China mediation: the United Kingdom and Japan position themselves as pro-safety norm advocates; France describes itself as a 'point of equilibrium' mediating between U.S. and Chinese blocs; Singapore seeks to actively promote model evaluation interoperability. These roles are undermined by normative fragmentation between countries - the U.K. and Japan are increasingly aligned with a hawkish U.S. attitude towards China, as opposed to France's cooperation and Switzerland and the U.A.E's signalled neutrality. While economic competitiveness is a shared strategic ambition of each nation, this tends to be characterised in different ways (technological sovereignty, increased foreign investment, digital market interoperability), and does not clearly align with strengthened pro-safety regulation.

There is a moderate degree of political will for international governance efforts, as indicated by extensive middle power participation in AI Safety Summits, U.N. Global Dialogues on AI Governance, International Dialogues on AI Safety, The International Network of AISIs, the OECD, GPAI and Hiroshima Process Networks, and the ISO/IEC JTC 1/SC 42 subcommittee and UN/ITU joint evaluation projects. Support for binding international treaties, however, is low, as indicated by the widespread preference for voluntary governance schemes at domestic and regional levels. This suggests that either a focussing event or concentrated advocacy and coordination may be needed to generate political will for binding commitments.

Aside from normative unity and political will, the effectiveness of middle power deceleration mechanisms depends on the extent to which both superpowers are willing to participate in international governance initiatives. While a full analysis is beyond the scope of this report, several indications of Chinese willingness should be noted. China signed the Bletchley, Seoul, and Paris declarations, and contributed to the inaugural International AI Safety Report. Chinese government publications suggest a high level of willingness to participate in threat information sharing between special technical institutions, as well as support for the creation of shared technical standards (2025 National AI Safety Governance Framework 2.0, p. 59). Chinese experts already participate as part of an international epistemic community through the International Dialogues on AI Safety (2025 IDAIS-Shanghai Statement). While China is not formally a member of the AISI Network, CnAISDA's evaluative procedures have converged with recent benchmarks (LiveSecBench, and ForesightSafety Bench 2026). China's Global AI Governance Initiative welcomes stakeholders 'to jointly promote the governance of AI under the principles of extensive consultation, joint contribution, and shared benefits.' CnAISDA's 2025 Initiative on Promoting International Cooperation on AI Safety and Inclusive Development strongly advocates greater international coordination. Concretely, China's Action Plan calls for 'the development of an open-source compliance system.' Given that the nation has openly stated an interest in 'the establishment of open platforms to share best practices and promote international cooperation on AI safety governance worldwide,' Chinese willingness to participate in U.N.-backed international governance initiatives may be higher than hawkish narratives typically suggest.

The thematic analysis of policy documents has produced a complex picture. Although there likely is a moderately high degree of political will for the deceleration of U.S.-China frontier AI race dynamics, this does not currently extend to binding international commitments, sanctions-based regulation, or moratoria. Further, while AI safety and the prevention of catastrophic risks is a notable concern of several middle powers, this is not to imply a high level of normative cohesion, and fault-lines exist concerning attitudes towards China. Neither political will nor normative unity are static variables, and both may increase given external focussing events, domestic pressure from concerned citizens, and international policy advocacy campaigns.

Several pathways of future research would be valuable. Further middle powers could be analysed and compared - for instance, Russia, India, Canada, Israel, and Saudi Arabia, and the results of this thematic analysis could be validated through semi-structured interviews held with policy-makers and government officials. Finally, the effectiveness of aforementioned windows of opportunity - the 2027 and 2028 summits, as well as future technical working groups hosted by the International Network of AI Safety Institutes - could be evaluated through stakeholder consultations.

References

Albous, M.R., Al-Jayyousi, O.R. and Stephens, M. (2025) 'AI Governance in the GCC States: A Comparative Analysis of National AI Strategies', *Journal of Artificial Intelligence Research*, 82, pp. 2389–2422. DOI: 10.1613/jair.1.17619.

Allen, G.C. and Adamson, G. (2024) *The AI Safety Institute International Network: Next Steps and Recommendations*. Washington, D.C.: Center for Strategic and International Studies, 30 October. Available at: https://www.csis.org/analysis/ai-safety-institute-international-network-next-steps-and-recommendations

Allen, J.G. and Liao, Q.X.M. (2025) 'Digital Economy Innovation in the Indo-Pacific: Towards a "Singapore Effect"?', *Journal of World Investment and Trade*, 26(4), pp. 680–711.

Amadori, A., Alfour, G., Miotti, A. and Behrens, E. (2025) 'How Middle Powers May Prevent the Development of Artificial Superintelligence'. SSRN Working Paper. Available at: https://ssrn.com/abstract=5776982

Bengio, Y. et al. (2024) 'Managing Extreme AI Risks Amid Rapid Progress', *Science*, 384(6698), pp. 842–845. DOI: 10.1126/science.adn0117.

Buhl, M.D., Bucknall, B. and Masterson, T. (2025) 'Emerging Practices in Frontier AI Safety Frameworks'. arXiv:2503.04746. Available at: https://arxiv.org/abs/2503.04746.

Cave, S. and ÓhÉigeartaigh, S.S. (2018) 'An AI Race for Strategic Advantage: Rhetoric and Risks', in *Proceedings of the 2018 AAAI/ACM Conference on AI, Ethics, and Society (AIES '18)*, New Orleans, LA, 2–3 February. New York: ACM, pp. 36–40. DOI: 10.1145/3278721.3278780.

Cheng, J.H., Chong, B. and Gomez, M.A. (2026a) 'Strategic Choices for Middle Powers in Developing AI Capabilities: A Case Study of Singapore', *Asian Security*, 22(1). DOI: 10.1080/14799855.2025.2581269.

Chin, Y.C., Raho, D.A., Kim, H.-M., Bi, C., Ong, J., Huang, J. and Stinckwich, S. (2026) 'Interoperability in AI Safety Governance: Ethics, Regulations, and Standards'. arXiv:2601.06153. Available at: https://arxiv.org/abs/2601.06153.

Cihon, P. (2019) *Standards for AI Governance: International Standards to Enable Global Coordination in AI Research & Development*. Technical Report. Oxford: Centre for the Governance of AI, Future of

Humanity Institute, University of Oxford. Available at: https://www.fhi.ox.ac.uk/wp-content/uploads/Standards_-FHI-Technical-Report.pdf.

DETEC (2025) 'Switzerland to Host a Global Summit on Artificial Intelligence in 2027'. Press Release, Federal Department of the Environment, Transport, Energy and Communications, 25 June. Available at: https://www.uvek.admin.ch/en/newnsb/qewY8BHWPhcMQEYV12fkr.

Dung, L. and Hellrigel-Holderbaum, M. (2025) 'Against Racing to AGI: Cooperation, Deterrence, and Catastrophic Risks'. Available at: https://philarchive.org/rec/LEOART-3.

Eslami, M., Vieira, A., Adib-Moghaddam, A., Borges, L., Papageorgiou, M., Cristiano, F., Al-Marashi, I., Sauer, T. and Kaunert, C. (2025) 'The Geopolitics of AI-Driven Arms Races', *Geopolitics* [Online first, 28 October]. DOI: 10.1080/14650045.2025.2572695.

Flink, T. and Schreiterer, U. (2010) 'Science Diplomacy at the Intersection of S&T Policies and Foreign Affairs: Toward a Typology of National Approaches', *Science and Public Policy*, 37(9), pp. 665–677. DOI: 10.3152/030234210X12778118264530.

Fort, K. (2024) 'The Role of AI Safety Institutes in Contributing to International Standards for Frontier AI Safety'. arXiv:2409.11314. Available at: https://arxiv.org/abs/2409.11314.

Katzke, C. and Futerman, G. (2024) 'The Manhattan Trap: Why a Race to Artificial Superintelligence is Self-Defeating'. arXiv:2501.14749. Available at: https://arxiv.org/abs/2501.14749.

Pavel, B., Ke, I., Smith, G., Brown-Heidenreich, S., Sabbag, L., Acharya, A. and Mahmood, Y. (2025) *How Artificial General Intelligence Could Affect the Rise and Fall of Nations: Visions for Potential AGI Futures*. Santa Monica, CA: RAND Corporation, RRA3034-2, 2 July. Available at: https://www.rand.org/pubs/research_reports/RRA3034-2.html.

Ryan, F., Iliadis, N. and Guest, O. (2024) *Weaving a Safety Net: AISI Collaboration*. Report. The Future Society, November. Available at: https://thefuturesociety.org/wp-content/uploads/2024/11/Weaving-a-Safety-Net_AISI-Collaboration_November-2024.pdf.

Sandoval, F.J.V. and Wilkinson, I. (2026) *How Middle Powers Can Weather US and Chinese AI Dominance*. London: Chatham House, 16 February. ISBN: 978 1 78413 671 0. Available at: https://www.chathamhouse.org/2026/02/how-middle-powers-can-weather-us-and-chinese-ai-dominance.

Schmid, S., Lambach, D., Diehl, C. and Reuter, C. (2025) 'Arms Race or Innovation Race? Geopolitical AI Development', *Geopolitics*, 30(4), pp. 1907–1936. DOI: 10.1080/14650045.2025.2456019.

Schwarz, E. (2025) 'From Blitzkrieg to Blitzscaling: Assessing the Impact of Venture Capital Dynamics on Military Norms', *Finance and Society*, pp. 1–24. DOI: 10.1017/fas.2024.18.

Singer, S., Elmgren, K. and Guest, O. (2025) *How Some of China's Top AI Thinkers Built Their Own AI Safety Institute*. Washington, D.C.: Carnegie Endowment for International Peace, June. Available at: https://carnegieendowment.org/russia-eurasia/research/2025/06/how-some-of-chinas-top-ai-thinkers-built-their-own-ai-safety-institute.

Sytsma, T. (2026) *Decisive Economic Advantage: Modeling the Transition from Temporary First-Mover Leads to Economic Dominance in Artificial General Intelligence*. Santa Monica, CA: RAND Corporation, RR-A4444-1. Available at: https://www.rand.org/pubs/research_reports/RRA4444-1.html

Tran, H.-C. (2026) 'Brokerage in the Black Box: Swing States, Strategic Ambiguity, and the Global Politics of AI Governance'. arXiv:2601.06412. Available at: https://arxiv.org/abs/2601.06412.

Valeriani, M. and Polito, C. (2025) 'From Host to Actor? Italy's Foreign Policy Strategy on Artificial Intelligence at the G7', *Contemporary Italian Politics*, 17(4), pp. 452–464. DOI: 10.1080/23248823.2025.2556627.

Velasco, L., Trager, R. et al. (2025) *The Future of the AI Summit Series*. Oxford: Oxford Martin AI Governance Initiative. arXiv:2601.02383. Available at: https://arxiv.org/abs/2601.02383.

Wang, A.H.-E. and Siler-Evans, K. (2026) *U.S.-China Competition for Artificial Intelligence Markets: Analyzing Global Use Patterns of Large Language Models*. Santa Monica, CA: RAND Corporation, 14 January. Available at: https://www.rand.org/pubs/research_reports/.