



Who Controls AI? Nationalising Trust in the Indo-Pacific and Beyond

By Max Cappuccio

Intelligent technologies cannot be effectively governed in the absence of public trust. In Western societies, public anxiety about AI is typically construed as the fear that humans may become unable to control intelligent machines and their societal effects. But people do not fear AI simply because it is powerful; they distrust the organisations that develop, own, and decide how to use that power. Trust reflects less technological literacy than confidence in government, private enterprise, national development narratives, and the authorities expected to manage technological risks.

Cultural specificities influence how nationally coordinated AI programs are perceived, soliciting greater or smaller appetites for state-directed interventions for technology development and adoption,

industry centralisation, and infrastructure control. Western publics prevalently tend to foreground privacy, dignity, employment, and democratic accountability; East Asian debates often give greater weight to technical reliability, collective security, social coordination, and national capability.

Confidence in AI is significantly higher in China, India, Singapore, and parts of Southeast Asia than in the United States, Australia, Japan, and most European countries. These trust differences are especially relevant in the Indo-Pacific, where national AI programmes reflect different political economies, innovation ecosystems, cultural narratives, and geostrategic ambitions.

Trust tends to decrease wherever AI ambition is perceived as an expression of corporations

inherently geared toward profit maximisation, market dominance, data extraction, labour reduction, and political influence. Because private agendas need not reflect sovereign goals or answer public concerns, fear of AI is engendered by distrust of the socio-technical and politico-economic systems influenced by corporate power. Before asking whether AI is safe or reliable, the public asks who governs it, who benefits, and who bears the risks.

Conflicting and opaque narratives increase their distrust. Workers are told that automation will raise productivity but are rarely assured that it will improve job security or working conditions.

Professionals are sold tools trained on their knowledge and designed to monitor, deskill, or replace them. Citizens encounter facial recognition, behavioural prediction, and mass-surveillance from the same systems entrusted with their security. The prevalent fear is not that machines will escape control, but that private actors will control them to pursue goals that do not represent public values, tailoring AI to their own interests.

This is why ethical discourse alone often fails to generate trust. Corporate commitments to fairness, transparency, privacy, responsibility, and human-centred design **remain abstract** when disconnected from ownership, labour protection, democratic oversight, and social justice. Ethics washing occurs when institutions debate how AI should behave while excluding who should control AI and what purposes it should serve. A company may

adopt an ethics charter while automating employment, appropriating data, expanding surveillance, lobbying against regulation, or controlling strategic infrastructure.

These concerns intensify when technology firms exert influence over the defence institutions they work for/with. Autonomous weapons, decision-support systems, cyber capabilities, and surveillance technologies are prevalently developed within dual-use ecosystems integrating civilian industry, universities, intelligence agencies, and armed forces. In this context, companies involved in cloud computing, data analytics, autonomous systems, and generative AI are no longer merely suppliers. Some present themselves as strategic actors responsible for national security, capacity resilience, and military superiority. Recent controversies surrounding **Palantir** and **Anthropic** illustrate this shift. Palantir's leadership portrays technological development as politically non-neutral and links innovation to hard power, civilisational competition, and military recruitment. **Critics interpret this as an attempt to elevate corporate-state power over democratic deliberation**, observing that major firms are moving from supplying technical means to defining political ends.

Proposals to nationalise AI, or to place critical parts of its infrastructure under public ownership and strategic direction, respond directly to this anxiety. Nationalisation reduces neither to expropriation nor to centralisation of productive capabilities, but it may implicate public equity, sovereign wealth funds, state compute infrastructure,

strategic procurement, binding access requirements, or government-led coordination of research and development. These arrangements differ in purpose, but all recognise that AI has become too consequential to be treated as an ordinary private commodity.

Three approaches illustrate the range.

Bernie Sanders's social-democratic model would acquire a substantial public stake in leading AI companies through a sovereign wealth fund, giving citizens voting power and a share of the wealth generated by automation. **Donald Trump's nationalist approach** is less concerned with redistribution than with strategic leverage: public stakes, procurement power, and negotiated partnerships would align frontier firms with national industrial, security, and geopolitical objectives. **Xi Jinping's five-year plan** is more comprehensive and integrates **political governance**, public investment, universities, private enterprise, and military-civil fusion within a long-term programme of national modernisation and **capability expansion**.

East Asian countries have spearheaded state programmes that embed AI development within coordinated industrial, research, and security strategies. Their approaches, however, have diverged.

In China, AI is presented as part of societal modernisation, strategic sovereignty, administrative coordination, and military transformation, with ample space for private entrepreneurship and decentralised

capabilities. Its development is embedded in a close relationship among central and local governments, universities, private enterprises, and the armed forces. Public optimism may therefore be linked to the expectation that corporate goals must align with a broader political vision and national values. This model can accelerate capability development and reduce foreign dependence, but some Western commentators have raised concerns about surveillance, authoritarian control, aggressive militarisation, and the subordination of individual rights to state-defined goals.

South Korea offers a **developmental-security model**. AI is connected to economic growth, technological leadership, demographic pressures, and the continuing threat from North Korea. State-supported firms, research institutions, and defence organisations treat autonomous systems as force multipliers capable of compensating for personnel shortages, strengthening deterrence, and supporting a globally **competitive defence industry**. Legitimacy and trust are primarily associated with competence, preparedness, strategic necessity, and technological reliability but also with cultural cohesiveness.

In Japan, demographic anxieties, cultural familiarity with robots and narratives presenting machines as companions and co-workers coexist with constitutional constraints that limit dual-use solutions. Narratives stressing a presumed affinity of Japanese people for robotics **don't necessarily reflect unrestricted acceptance** and have often

been mobilised to support divisive policies, including the [adoption of robots in eldercare](#) and as a response to labour scarcity. Japan therefore shows that cultural familiarity and national need can't assure public legitimacy if citizens distrust their institutions.

These cases suggest that the regional AI race has encouraged strategic synergies among governments, corporations, universities, and defence institutions. Globally, nationalisation may contribute to establish similar synergies using different solutions, ranging from public equity and sovereign funds to state-led research programs and military-civil coordination. Each redistributes authority differently.

Integrated ecosystems can win popular trust insofar as they make technological power publicly accountable, politically contestable, and directed toward collective goals such as social stability, human flourishing, strategic autonomy, and protection of identities.

Public involvement can increase trust when it makes the benefits of innovation tangible, protects employment and public services, and gives citizens or national institutions meaningful influence over technological priorities.

Military leaderships appreciate national programmes' strategic advantages: sovereign access to compute, data, models, cloud infrastructure, testing facilities, and skilled personnel; continuity of service during

crises; stronger supply-chain security; and reduced dependence on foreign vendors whose commercial or political decisions may constrain national action. Owning a weapon platform is insufficient if the decisive model, data pipeline, cloud layer, or update process remains controlled by a foreign or unaccountable contractor. This contributes to explain why military AI has yet to fully gain the trust of citizens, [service members](#), and [military leaderships](#). National programs may help mitigate their concerns, preserving sovereign access, auditability, operational continuity, and freedom from vendor lock-in.

Yet nationalisation is not automatically ethical, let alone democratic. Without transparency, contestability, and institutional checks, nationalisation may [“accelerate the corporate-government fusion we’re already sliding toward,”](#) promoting state monopolies that pursue surveillance and militarisation without factually reducing tech oligarchies' influence. State ownership is not rewarding in itself but only insofar as it promotes publicly accountable technological sovereignty.

Nationalising trust, not merely assets, will prove key to secure sovereign capability while ensuring that technological power remains politically legitimate, socially beneficial, and open to public scrutiny.

Dr Massimiliano (Max) Cappuccio currently is a senior researcher affiliated with the Creative Robotics Lab of UNSW Sydney.