Governing with Machines: Statesman's Quest

Mordechai Katash

January 2025

Every generation inherits a set of tools that quietly rewires what it means to lead. The printing press expanded literacy, the steam engine expanded power, and the internet expanded reach; ***Artificial Intelligence (AI) expands clarity of thought****. For the first time, societies can industrialise cognition itself, compressing weeks of analysis into minutes, translating oceans of data into decisions, and moving the "centre of gravity" from physical assets to computational advantage. The question is no longer whether AI will be incorporated into our lives, but on whose terms, under what rules, and toward what ends.*

In my earlier work, ***"Artificial Intelligence = Clarity of Thought",*** *a chapter I contributed in the book: "Artificial Intelligence versus Actual Intelligence" (August 2025), I framed AI as an amplifier of human reasoning: a capability that can elevate decision quality when anchored to discipline, ethics, and purpose.*

This chapter extends that idea into the ***"Domain of Statecraft"****. A statesman does not merely adopt technology; he or she integrates it into national policy, legislation, and funding in a way that preserves sovereignty, strengthens resilience, and protects human dignity. The framework presented here is intentionally simple. If AI is becoming a national capability, then the state must treat it as it treats all strategic capabilities: it must* ***defend*** *with it,* ***build*** *with it, and* ***finance*** *with it. These three pillars:* ***AI Defence, AI Infrastructure,*** *and* ***AI Finance****, form a practical doctrine for incorporating AI into national life without surrendering the human core of governance.*

The Statesman and the Machine: Defining a National AI Ethos

AI is frequently discussed as a product category (tools, platforms, models), yet for governments it functions more like a strategic layer that sits across every domain: security, education, energy, healthcare, industry, and markets. The state's task is therefore to define an "AI ethos" that aligns technological capability with national values. Absent such an ethos, AI adoption becomes fragmented, driven by procurement cycles, vendor narratives, or short-term political incentives.

An AI ethos should answer three questions:

1. What must remain human (accountability, lawful authority, moral judgement)?
2. What can be delegated to machines (pattern detection, forecasting, optimisation, routine compliance)?
3. How do we structure oversight so that machine speed does not erode democratic legitimacy?

Modern AI systems can generate outputs that are highly persuasive but not necessarily accurate, and they can optimise objectives in ways that produce unintended externalities. The statesman must therefore insist on transparency, testability, and auditable decision trails, particularly where rights, safety, and public trust are implicated (Floridi et al., 2018). Operationally, an AI ethos is expressed through policy instruments: national AI strategies, risk-based regulation, data governance, public-sector capability building, and funding

priorities for research and commercialisation. It is also expressed through a “public narrative” that invites citizens to understand where AI will be used, why it is being used, and how harm is prevented. Trust becomes an asset class of its own. In the AI era, legitimacy is not a communications strategy, it is a governance system.

AI Defence: Asymmetry, Autonomy, and Ethical Warfare

Defence is the first pillar because security is the precondition of prosperity. In contemporary conflict, asymmetry often outweighs scale. Smaller actors can inflict outsized damage through cyber operations, disinformation campaigns, and attacks on critical infrastructure. AI increases both the velocity and the ambiguity of these threats, enabling adversaries to automate reconnaissance, generate persuasive propaganda at scale, and probe systems continuously for weaknesses.

AI Defence therefore begins with the recognition that the “era of weaponry” has expanded into an era of cognition. Decision advantage: the ability to observe, orient, decide, and act faster than an opponent, becomes a decisive capability. Machine learning can assist by correlating signals across cyber telemetry, communications, logistics, and open-source intelligence, producing actionable threat assessments in near real time (Russell and Norvig, 2020).

A statesman’s AI Defence agenda should typically include:

1. resilient cyber posture (AI-enabled detection, automated response, and continuous redteaming)
2. disinformation resilience (content provenance, civic media literacy, and rapid countermessaging).
3. secure supply chains for chips, cloud, and communications.
4. clear rules of engagement for autonomous systems. The aim is not automation for its own sake; it is controllable capability that strengthens deterrence.

This brings us to a paradox: in the AI era, offence is often delivered via defence. Adaptive defence systems learn from every attempted breach, hardening over time and raising the cost of attack. However, as autonomy increases, so does the risk of unintended escalation. The ethical boundary between “defensive autonomy” and “pre-emptive aggression” can blur quickly when systems are empowered to act at machine speed. For this reason, human-inthe-loop (or, at minimum, human-on-the-loop) oversight should be mandatory for decisions involving lethal force or significant rights impacts. Risk-based frameworks and governance mechanisms, similar in spirit to the NIST AI Risk Management Framework, are essential to keep capability aligned with lawful authority and public accountability (NIST, 2023).

AI Infrastructure: Building the Intelligent Nation

If defence protects the nation, **infrastructure builds it.** AI infrastructure is not limited to data centres; it includes the full stack that enables intelligent capability: compute, data, connectivity, energy, standards, and skills. Nations that treat AI as a mere “software layer” will quickly discover that their dependence on external compute and proprietary platforms becomes a sovereignty risk. Conversely, nations that invest intelligently can build an “intelligent republic” in which public services become more personalised, efficient, and equitable.

A practical starting point is smart economic development. Governments can deploy AI to reduce friction in service delivery (licensing, compliance, benefits processing), to optimise infrastructure planning (communication, transport, energy, water, housing), and to support industry productivity (manufacturing, logistics, agriculture). Yet these benefits require a disciplined approach to data governance: clear data ownership, consent, privacy protections, and secure sharing mechanisms. High-risk applications should be subject to proportionate safeguards and transparency obligations, consistent with the risk-based direction of the European Union's AI Act (European Commission, 2021).

The second infrastructure principle is to **turning weakness into strength**. Constraints, such as: geography, population size, resource scarcity, agriculture, can become catalysts for focused innovation. A smaller nation can be faster to legislate, quicker to pilot public sector use cases, and more agile in coordinating universities, industry, and government. It can also specialise: for example, in secure digital identity, regtech (Regulatory Technology), AI enabled health diagnostics, or climate analytics. In such a model, sovereignty is achieved not through scale, but through precision and coherence.

The third principle is the **slingshot of innovation**. AI-driven growth accelerates where talent, data, and incentives align. Governments can act as "market shapers" by funding research translation, procuring innovative solutions, and setting standards that reward safety and interoperability. Strategic investments in education matter here: citizens must be AI literate, and public servants must understand procurement, evaluation, and risk controls for AI systems. At a technical level, continued advances in deep learning and representation learning remain central to capability, reinforcing the value of sustained research and workforce development (LeCun, Bengio and Hinton, 2015).

AI Finance: Dynamic Capital in the Algorithmic Age

Finance is the **bloodstream of national capability**. AI is transforming finance not only through automation but through a shift from static models to adaptive intelligence. Modern Portfolio Theory (MPT) provided a foundational framework for diversification, yet it rests on assumptions that weaken in a world of algorithmic trading, instantaneous information diffusion, and fat-tailed volatility. Markets now move as networks: correlations shift rapidly under stress, and narrative can reprice assets in hours.

This context gives rise to Dynamic Portfolio Intelligence: systems that continuously learn from market microstructure, cross-asset signals, macroeconomic data, and sentiment. Such systems can rebalance portfolios based on changing regimes rather than fixed historical parameters. Used wisely, this can enhance risk management for institutions, pension funds, and sovereign wealth strategies. Used poorly, it can amplify systemic risk if many actors converge on similar models and signals.

Here the statesman's role is twofold. First, to modernise regulation so that AI in finance is transparent, resilient, and auditable. Second, to ensure that national capability is developed through talent, data standards, and responsible experimentation. The rise of fintech and regtech illustrates how regulators themselves can use AI to detect fraud, monitor conduct, and anticipate emerging risks, provided they invest in capability and governance (Arner, Barberis and Buckley, 2017).

Finally, the way I phrase it: **“Fibonacci on steroids”,** is a useful metaphor for what AI does to pattern recognition. Financial markets have always been studied through cycles, ratios, and behavioural dynamics; AI multiplies the dimensionality of this analysis, detecting relationships across timeframes, instruments, and narratives that exceed human bandwidth. The point is not to mystify markets, but to acknowledge that capital now moves through informational ecosystems that reward speed, learning, and disciplined risk controls. Nations that understand this shift can better steward retirement savings, design resilient financial regulation, and manage the macroeconomic feedback loops that arise when algorithms become major market participants.

Ethics, Governance, and Human Centricity

No doctrine for incorporating AI is credible without ethics. AI systems can encode bias, erode privacy, and concentrate power. They can also degrade the quality of public discourse when misinformation becomes cheap to produce and difficult to authenticate. Ethical governance must therefore be operational, not rhetorical. It requires defined roles, measurable controls, independent assurance, and clear lines of accountability.

At minimum, states should adopt a risk-tiered model that distinguishes low-risk productivity applications from high-risk systems that affect rights, safety, or essential services. High-risk use should require stronger obligations: data quality standards, explainability, human oversight, impact assessment, and ongoing monitoring. Such principles are consistent with leading ethics frameworks and emerging regulatory approaches (Floridi et al., 2018; European Commission, 2021).

Human centricity is not an argument against AI; it is a design requirement. The objective is to ensure that AI increases human capability and institutional integrity rather than replacing judgement or weakening responsibility. In practical terms, this means investing in:

1. evaluation and audit capability.
2. public transparency and contestability.
3. education that equips citizens to understand, question, and responsibly use AI in their own lives.

Incorporating AI into our lives is not a technical upgrade; it is a civilisational choice. It asks governments to modernise how they defend their people, how they build national capability, and how they steward capital in a world where cognition itself has become industrial. The statesman’s challenge is to move beyond slogans, neither fearfully rejecting AI nor uncritically adopting it, and instead to create a coherent doctrine of capability and restraint. If the twentieth century-built nations on steel, oil, and credit, the twenty-first will build them on compute, data, and trust. AI will reward societies that can combine velocity with virtue, systems with conscience, power with restraint and innovation with accountability. The statesman of the AI era is therefore not merely a technocrat, but a steward: one who uses machines to illuminate decisions while keeping the human being, and the moral law, at the centre of the republic.

References

Arner, D.W., Barberis, J. and Buckley, R.P., 2017. Fintech and regtech: Impact on regulators and banks. Journal of Banking Regulation, 19(4), pp. 1-14.

European Commission, 2021. Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Brussels: European Commission.

Floridi, L. et al., 2018. AI4People - An ethical framework for a good AI society: Opportunities, risks, principles, and recommendations. Minds and Machines, 28(4), pp. 689-707.

LeCun, Y., Bengio, Y. and Hinton, G., 2015. Deep learning. Nature, 521(7553), pp. 436-444.

National Institute of Standards and Technology (NIST), 2023. AI Risk Management Framework (AI RMF 1.0). Gaithersburg, MD: NIST.

Russell, S. and Norvig, P., 2020. Artificial Intelligence: A Modern Approach. 4th ed. Pearson.

Katash, M., 2025. Artificial Intelligence = Clarity of Thought. In: AI vs Actual Intelligence. AGE Publications.

Mordechai Katash is a former Associate Program Director at *Group Colleges Australia* and currently a MBus lecturer at *Polytechnic Institute Australia* (Melbourne)