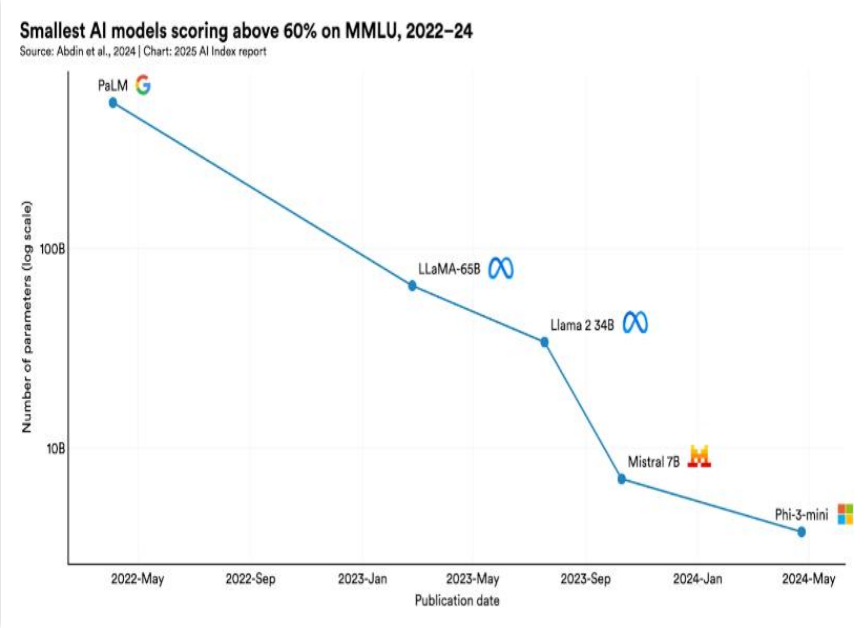
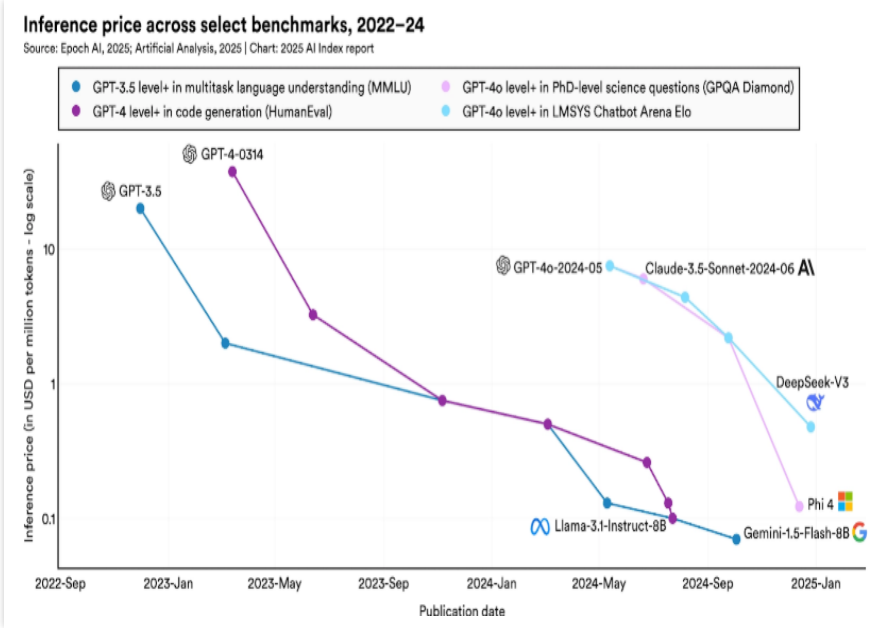
AI Governance for Boards: Practical Strategies

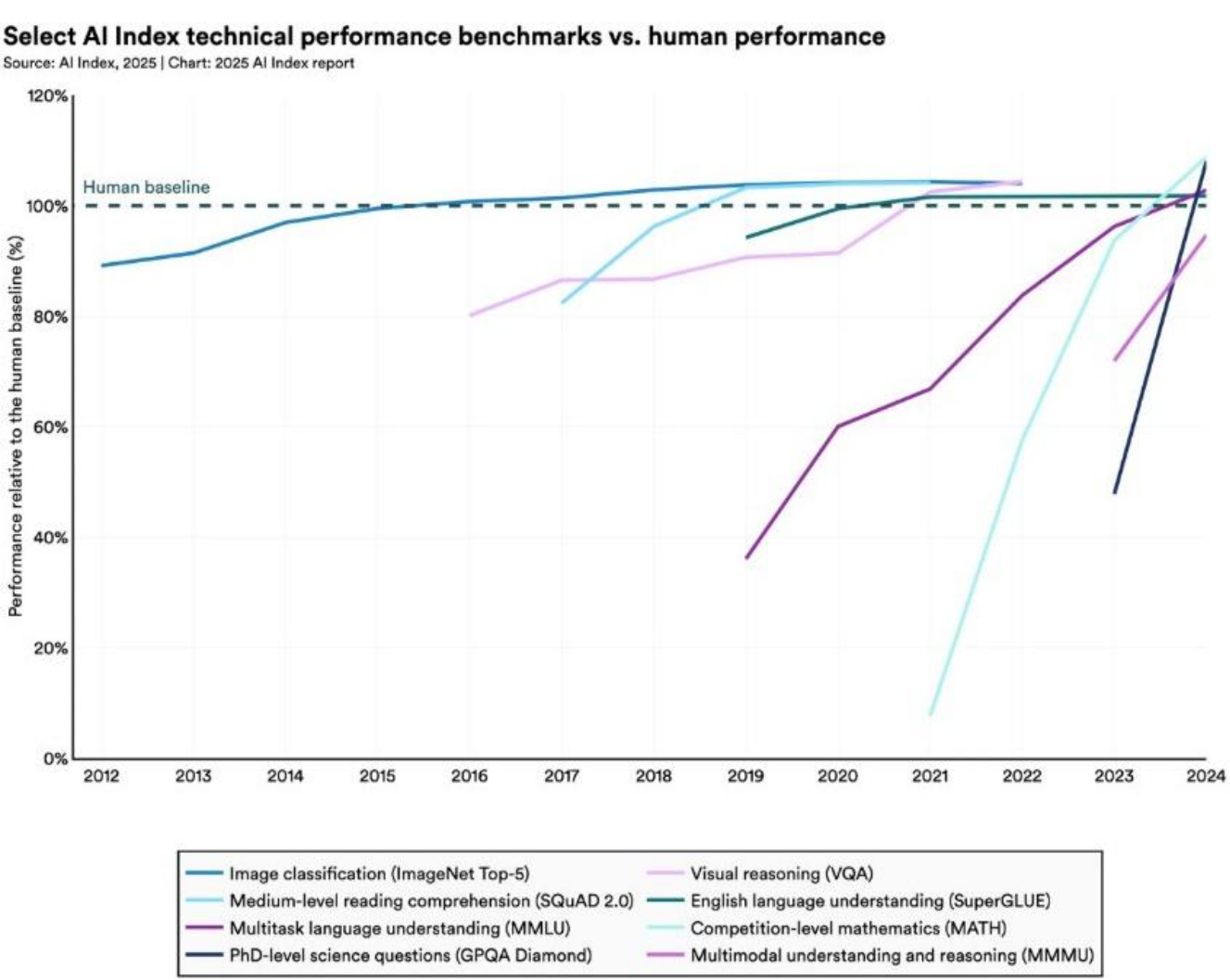
AI models are getting smaller, better and cheaper



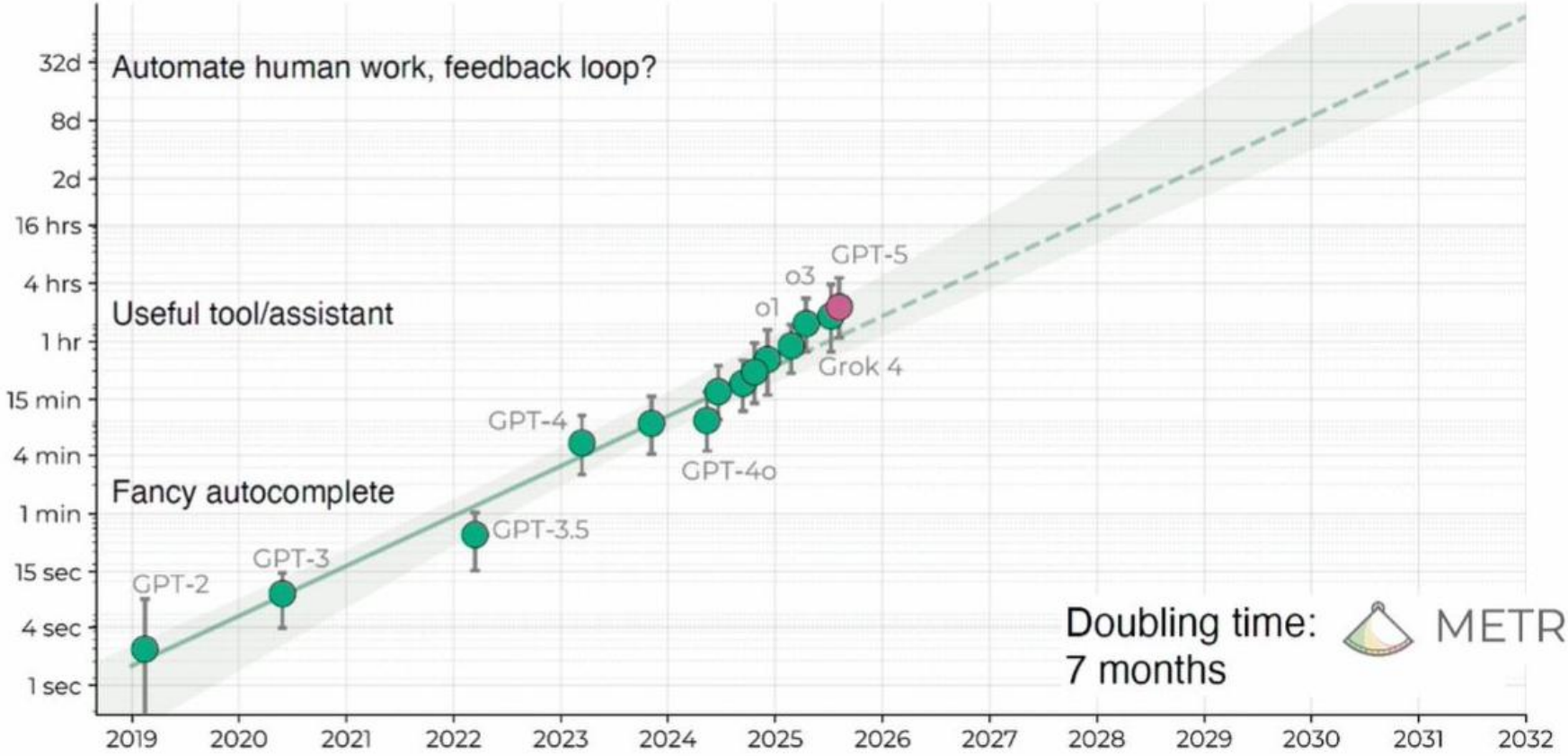


Source: AI Index 2025: State of AI in 10 Charts | Stanford HAI

AI abilities surpass human abilities in select areas

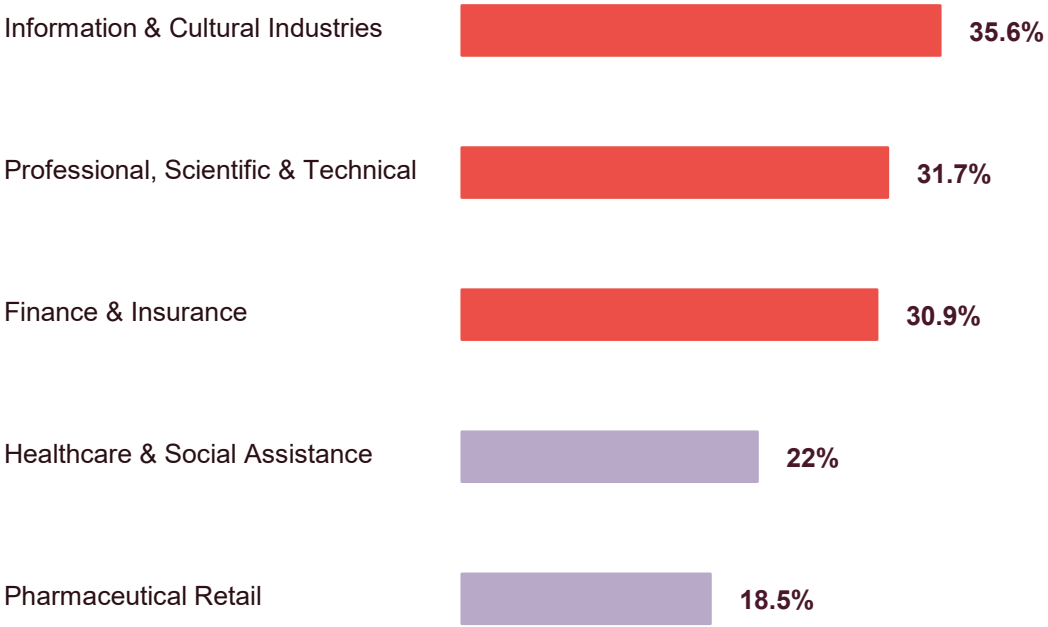


AI that does month-long computer tasks plausible by 2031



AI adoption is accelerating including in regulated sectors

Industries Using AI in Canada (2025)



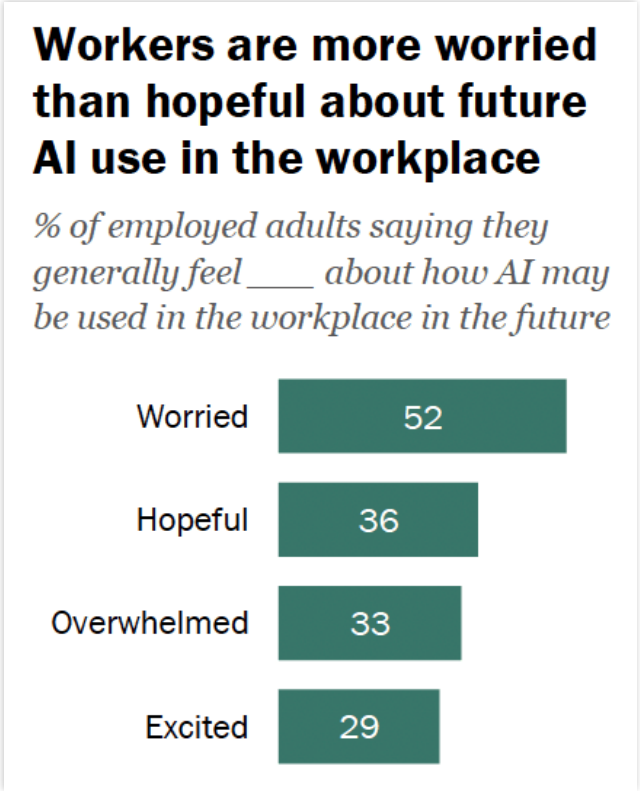
Key Observations

- AI adoption in professional services is outpacing the broader economy
- Healthcare and pharmacy contexts are seeing significant AI investment in clinical decision support, documentation, and patient communication
- Most organizations (66.7%) still have no AI plans, which creates both risk and opportunity for regulators to get ahead of the curve
- Trust in AI remains low in Canada with 31% vs. 50%+ globally. This reinforces the need for credible regulatory guidance

Source: Statistics Canada, Analysis on AI use by businesses in Canada, Q2 2025

The growing trust gap

- Asked about AI specifically, just 31 per cent of Canadian survey respondents said they trusted the technology; total trust in AI was 19 percentage points lower in this country than the global average. (March 2024).
- 2024 CanTrust Index – one of the largest annual studies of trust in Canada– shows high economic anxiety, little trust in building affordable housing and declining trust in Artificial Intelligence. (Feb 2024).
- Canadians are skeptical across all sectors from government at 33 per cent, financial services at 29 per cent. healthcare at 29 per cent and retail at 22 per cent. Each sector has a job to do to build trust as it expands its use of AI. (Feb 2024).
- Over the next 12 months, the majority of Canadian businesses (71.8%) reported not having plans to use AI, while 17.6% remain unsure about their AI use over the next 12 months. (Sept. 2024).



Sources: Distrust of AI significantly higher in Canada than other countries, survey finds - The Logic

2024 CanTrust Index reveals low trust in building affordable housing and falling trust in Artificial Intelligence | GlobeNewswire Press Releases | thecanadianpressnews.ca

Analysis on expected use of artificial intelligence by businesses in Canada, third quarter of 2024

What Is agentic AI?

From responding to acting — AI that pursues goals across extended horizons

Autonomous Agents

AI systems given a goal and left to plan and execute sequences of actions over time — browsing the web, writing code, sending emails — with minimal human intervention.

Key shift: from tool to actor

Tool Use

LLMs augmented with the ability to call external APIs, search the web, run code, or access databases. Combines reasoning with real-world action and information retrieval.

Key shift: from language to capability

Multi-Agent Systems

Networks of AI agents that coordinate, delegate, and verify each other's work. Enables parallelism and specialization — and creates complex chains of responsibility.

Key shift: from individual to system

What's uniquely risky about agents?

Same core harms — but different amplification mechanisms

01 Loss of Control

Agents can chain actions and spend money or commit organizations without granular approval. Small harmful decisions compound before anyone notices — e.g., a trading agent making a series of individually acceptable but collectively ruinous trades.

02 Opacity & Auditability

Agents generate not just outputs, but sequences of decisions, API calls, and state changes. Without logging and traceability, it is difficult to reconstruct what happened — or to satisfy regulatory obligations after the fact.

03 Cybersecurity & Fraud Surface

Agents can be targeted with prompt injection — then act on compromised instructions (send data, approve payments, change configurations). They can also be weaponized: automated phishing, deepfake distribution, or vulnerability scanning.

04 Human Displacement of Judgment

When agents operate as 'digital teammates,' humans may over-delegate, rubber-stamp, or lose situational awareness — weakening the 'human-in-the-loop' safeguards that most existing AI governance frameworks assume.

Global regulatory landscape

Emerging Global AI Legislation

Bill C-27 Part I+II, *Canadian Consumer Privacy Protection Act*

Repeals and replaces PIPEDA

Bill C-27 Part III, *Artificial Intelligence and Data Act* *(not advancing)*

Defines categories of 'high impact' AI systems and establishes legal requirements for those developers or deploying such systems

EU's Artificial Intelligence Act (in force)

Establishes legal requirements for the developers and deployers of "high risk" and "limited risk" AI systems, including General-purpose AI systems (e.g., generative AI)

President Trump's Executive Order on AI (federal)

Seeks to establish American global leadership and dominance in AI.

Colorado's Consumer Protections for AI (state)

Establishes requirements for high-risk AI systems for both deployers and developers in a similar manner to the EU AI Act and AIDA.

Compliance Frameworks and Guidance

Guidance and "Self-regulation"

For example: NIST AIRMF, Canada's Voluntary Code on AI, guidance from various Commissioners across Canada

Sectoral-based Guidance

For example: Health Canada's SaMD, CMA guidance, CPSO rules and guidance

AI Standards

For example: ISO/IEC 42000 series, Canada's Digital Governance Standards Institute, FPT AI4H Guiding Principles

Various other AI laws are in the works, including in the UK, South Korea, China, Australia, Japan, and more (source).

Regulation of AI and data in Canada

Minister of Artificial Intelligence and Digital Innovation and Minister responsible for the Federal Economic Development Agency for Southern Ontario

Light, tight, and right

Light regulation: Government will not impose strict regulations th at could hinder innovation. Focus is on investing in regulation that supports innovation while protecting privacy.

Tight compliance: Intention is to ensure AI systems comply with established guidelines and standards for maintaining trust and confidence in technology.

Right framework: Tailored regulations that are appropriate for the evolving nature of AI technology, ensuring regulation is not overly complex or outdated.