

The AI Harvest

How artificial intelligence is turning democratic openness into authoritarian advantage



Photography transformed military reconnaissance. Signals intelligence helped decide the Second World War. Satellite imagery defined the Cold War. Each breakthrough changed not just how intelligence was gathered, but what governments believed was knowable. Artificial intelligence is the next revolution in that lineage, and it will prove the most consequential of all.

What sets AI apart is its mechanism. Earlier breakthroughs widened collection by opening new frontiers. AI instead transforms the strategic value of information that already exists.

Every research paper, conference abstract, patent filing, procurement notice, academic collaboration, corporate disclosure, satellite image, professional profile and social media post adds another fragment to an immense digital mosaic. Individually mundane, these fragments resolve under frontier AI into patterns, relationships and strategic insights that no human analyst could assemble alone. This is the new frontier of "mosaic intelligence", and it is fast becoming the defining security challenge of our era.

For decades the West has rightly treated openness as a strategic asset. Liberal democracies prosper because ideas circulate freely, universities collaborate,

discoveries are published and markets stay transparent. Those same strengths now generate the richest intelligence environment ever assembled.

The contest has shifted from collection to correlation. Advantage no longer flows to whoever steals the most secrets, but to whoever extracts the most insight from what free societies publish by design. The nation that deploys the most capable analytical AI commands the geopolitical high ground.

Beijing has grasped this asymmetry and built for scale. Rather than relying on classical espionage alone, Chinese intelligence fuses frontier AI with the vast open records democracies generate - mapping supply chains, profiling institutions and targeting critical talent long before a human officer makes contact.

Human espionage now begins with machine triage. Earlier this month the Five Eyes alliance - the United States, United Kingdom, Canada, Australia and New Zealand - issued a rare joint warning that hostile services are using Western platforms such as LinkedIn, Indeed and Upwork as a primary targeting ground. The next step and the one that should worry us most is the marriage of that harvest to domestic AI: feed millions of scraped profiles into a capable model and you can map the internal hierarchies of Western defence contractors, identify researchers on sensitive dual-use programs, and isolate individuals with financial or personal vulnerabilities. The hostile recruiter no longer fishes in the dark; he arrives already knowing who holds access, influence and exploitable weakness.

In this landscape, Western frontier models are both weapon and prize. Anthropic alleged this month that operators affiliated with Alibaba ran some 28.8 million exchanges through roughly 25,000 fraudulent accounts to distil agentic reasoning and software-engineering capability from a leading Western model - a claim Alibaba denies. No firewall was breached; the model was used exactly as designed. Capability, once released, proves far harder to recall than to harvest. By interacting with our models, adversaries turn our own intellectual property into the training data for the very systems that will one day filter our open record.

This harvest is amplified by Beijing's doctrine of military-civil fusion, which blends research, industry and defence into a single instrument of state. Consider the Chinese Academy of Sciences. It runs more than 100 institutes, employs some 63,000 scientists and stands as the world's most prolific research publisher, while incubating national champions in semiconductors, quantum computing and AI. RAND Europe's recent directory identifies 17 CAS institutes as core defence partners of the People's Liberation Army - yet only three appear on the US entity list. An institution this powerful, this opaque and this militarised is a strategic actor, and Western security frameworks must treat it as one.

The pressure is already being felt across the Indo-Pacific, where analysts describe a pattern of "structural coercion": an environment in which asset extraction

becomes routine, while individual grey-zone operations are kept just below the threshold that would compel a decisive Western response.

Consider South Korea, a linchpin of the global technology supply chain. Korean authorities logged a sharp rise in technology-leak cases through 2025, with China behind most confirmed transfers of Samsung and SK Hynix semiconductor secrets - not disgruntled employees walking out with USB drives but coordinated campaigns to identify key engineers and target the precise proprietary processes Beijing's domestic chip industry needs. Seoul chose to harden its system: in February it extended its espionage statute beyond North Korea to encompass any foreign state. Hardening the legal and data ecosystem is a choice confident democracies can and must make.

There is a hard truth here for any democracy tempted to simply turn the same tools back on its rivals: the asymmetry does not reverse. Mosaic intelligence rewards whoever has the richest open record to mine, and authoritarian states offer far less of one. China censors and curates what crosses its borders; Russia and Iran marshal their information environments tightly; North Korea is very nearly a closed box. Where these states do publish at scale, much of it is shaped for foreign consumption - the sanitised foreign-language statement that signals far less ambition than its domestic-language original. Western analysts can train AI on the autocracies, but they will find thinner pickings, heavier deception and a far higher ratio of noise to signal. The open society is the rich seam; the closed society is the lean one. That imbalance is not a passing feature of the contest - it is the contest.

This asymmetry will only compound. While AI discovers patterns across today's datasets, the horizon brings quantum computing, which promises to accelerate correlation at scales prohibitive today. Together they will mine decades of accumulated public information, exposing structural relationships invisible to current systems. Every paper, procurement notice and digital interaction recorded today becomes a permanent deposit in tomorrow's hostile intelligence database. Democracies are building those databases in plain sight; our adversaries are learning to read them.

The answer, then, is mastery, not retreat - and not imitation either. Openness remains the West's decisive moral and economic advantage and surrendering it would simply hand authoritarian competitors a backdoor victory. The imperative is to govern openness as the strategic vulnerability it has become. Information governance is now national security. Corporate governance is now counter-intelligence. Boards that steward advanced technology are stewarding geopolitical assets; universities that train innovators are guarding research of immense strategic weight; governments that publish data for accountability must assume adversarial AI will aggregate the innocuous into the revealing.

For the Western democracies the stakes are sharpened, not softened, by the very things that make them strong: free universities, open capital markets, public



registers, a research culture that publishes by default. Each is a national asset and, increasingly, a national exposure. The instinct to manage that exposure by closing down would forfeit the one advantage worth defending.

This is no longer merely a cyber security challenge. It is an intelligence contest with new economics, and victory will favour the side that extracts the greatest strategic insight from what free societies willingly reveal - and builds the analytical power, and the human judgment to direct it, to do so first.

The first revolution taught governments to observe the battlefield. The second taught them to intercept the signal. The third taught them to see from orbit. Artificial intelligence is teaching them to understand everything. The democracies that intend to lead the coming decades must resolve to understand it best - and to act on what they learn.