

BRUSSELS ECONOMIC SECURITY REVIEW



The critical in critical technologies

by Bart Hogeveen

Emerging technologies were once treated as engines of prosperity. Today they are instruments of power. As global politics hardens and states weaponise technology for coercion, defence and strategic advantage, the question is no longer which technologies are critical but how nations manage foreign ownership, control and influence over the systems that now underpin their sovereignty.

Only a few years ago, governments viewed AI, quantum, biotech, advanced communications and robotics primarily as drivers of productivity and social benefit. By the mid 2020s, they had become assets to be protected: research to be ringfenced, firms to be shielded, intellectual property to be defended. Today, they are strategic positions within a globalised market where control over chokepoints, standards and supply chains confers geopolitical advantage.

Autonomy without illusions

An instinctive response to this shift is the pursuit of technological autonomy. While this impulse is visible across the United States, China, Europe and other advanced economies, only a few have the capacity to pursue it meaningfully. The United States and China benefit from large, deeply integrated domestic technology bases, built over decades and supported by markets of scale.

Most other economies lack these structural advantages. They are too small to replicate autonomy across all technology layers, too exposed to rely on market forces alone, and too dependent on foreign capital, intellectual property and infrastructure to dictate terms. For them, autonomy would take years to develop – if it is achievable at all – within a global technology ecosystem that is oligopolistic, globalised, highly competitive and fast-moving.

If autonomy is out of reach, the alternative is not naive trust but the active governance of dependency. This shifts the question from which sectors are strategic to which dependencies are critical as a function of trust, substitutability and control.

The question that actually matters

Consider a simple scenario. Your national digital identity system is operated by a foreign company. The firm is efficient, the technology is reliable, prices are competitive and its engineers are excellent. Is that a security problem?

The answer has little to do with the company's ownership or the quality of its products alone. It depends on who can reach into the layers that make up the system and direct how that system functions. If the answer is a foreign government with interests that are hostile to yours – and if the legal, technical and political architecture means you cannot prevent or even detect interference – then you have surrendered control of an artery of your national life.

This is the core insight of ASPI's In Whose Technology We Trust series. In reviewing how five Indo-Pacific democracies navigate the intersection of technology dependence and national security, the core finding is simple: the decisive variables are ownership, control and influence.

These variables are not hypothetical but real. Databases with our personal identifiable data are hosted abroad. Energy grids rely on proprietary software maintained remotely. Government data is stored in cloud infrastructures governed by foreign legal regimes. These dependencies become especially consequential when systems in question fall under foreign legal authority. They require active governance — and a redefinition of what trust means in a technologically interdependent world.

It's the stack, not the product

Public debate still imagines risk as a matter of product substitution: a Huawei router is replaced for Cisco, TikTok for ZigaZoo, WhatsApp for Signal and BYD for Tesla. Indeed, these are products seemingly easy to substitute. But modern digital infrastructure systems do not run on products. They run on stacks – intricate, interdependent layers of technology assembled from components sourced across the globe, often without the knowledge of the sellers or resellers deploying them.

A government agency's digital services could run on an American cloud platform, with data centres in the Gulf, which runs on semiconductors designed in the United Kingdom and manufactured in Taiwan, managed via

software whose components include open-source libraries maintained in China, updated remotely by engineers in multiple jurisdictions, through data centres across multiple sovereign territories.

These stacks are global, not American, Chinese or European per se. When you ban a vendor, you only address the visible layer. But the stack below it – the chips, firmware, cloud orchestration layer, software dependencies, legal jurisdiction governing remote access – may contain exposure just as significant, and far less visible.

Technology as deterrence, leverage and industrial policy

In a stable international environment, where alliances are durable, states act in accordance with agreed norms, legal frameworks are predictable and disputes are resolved within agreed rules, these dependencies might be tolerable. But the global order is no longer stable. States increasingly use technological capabilities as tools of deterrence, coercion and industrial strategy.

When Iranian drone strikes hit Autonomous Weapons Systems (AWS) data centres in the UAE and Bahrain in March 2026, the regime was not just notionally aware that digital infrastructure matters – they were actively targeting it. Iran named Microsoft, Google, Meta, Nvidia and other major technology companies as targets. Critically, the systems that proved most resilient were not the ones nationally controlled. They were the ones most intelligently distributed. Digital infrastructure is now a domain of power in its own right.

But the exercise of power through technology does not begin at the point of disruption. It is embedded in the structure of systems themselves. A persistent assumption in policy debates is that technology is neutral until it is misused – that risk arises only when malicious actors intervene. This view obscures how authority is already encoded in infrastructure. Systems are designed and embedded with assumptions about control, access and oversight.

The US–China technological race should be seen in that context too. Despite it often being framed as a competition for innovation, it is in fact a competition for technological dominance and asymmetrical dependencies. Those who dominate set the rules and conditions for how a technology is used and for the future direction of development. While the US may be the most visible and vocal actor, it is China we should watch the most intensely.

ASPI's Critical Technology Tracker shows how China over a 20-year period acquired a significant lead in research output across most of the emerging technologies that will form the foundation of tomorrow's stacks. Not just in manufacturing volume, but in intellectual property, standards-setting bodies and the supply of engineers trained at institutions with links to state security apparatus.

The risk of stack-based monopolies is not a present-day problem that can be solved by present-day bans. It is a forward accumulation of dependency being locked in right now, as the next generation of technology is designed, built and distributed.

Trust is the allocation of risk under uncertainty

This compels us to re-think our approach to 'trust'. Trust has been the primary language through which technological dependencies have been justified in policy. Think of conceptions like trusted vendors, trusted geographies, zero-trust network architecture and trustworthy AI. It implies a choice made under uncertainty: a willingness to rely on another actor despite the possibility of failure or betrayal. It assumes both awareness and reversibility. However, many technological relationships today lack both. In fact, most dependencies are better understood as acquiescence.

Yet, most of the dependencies now considered undesirable started as rational procurement decisions, presumably based on performance and price. While vendors may have offered contractual assurances, no amount of corporate goodwill can override legal obligations to compel cooperation with state objectives.

Moreover, trust and risk are neither stable nor fully knowable. It changes with political relations, regulatory regimes, and technological development. There is no fixed boundary between secure and insecure systems, and no definitive list of reliable suppliers.

Under these conditions, trust cannot function as a moral or value-driven judgment. It is better understood as a way of allocating risk across systems and relationships. To trust a technology is to accept that certain forms of failure are tolerable, while others are not; that some dependencies are manageable, while others create unacceptable exposure.

Yet public debate often oscillates between extremes: assuming that all foreign technology is inherently suspect or none of it is. Both approaches flatten important distinctions between systems, functions and levels of dependence. A more realistic approach begins from asymmetry.

Why 5G was the right call – and why it is now not enough

The 5G debate crystallised the issue of high-risk vendors. 5G telecommunications infrastructure did not only promise faster mobile connectivity, but it would form the nerve system through which a modern economy functions: financial transactions, emergency services, logistics, military communications and the data flows that underpin government itself. Foreign ownership, control or influence of that infrastructure provide the capability to monitor it, degrade it or shut it down – not only during times of conflict but at any moment of political coercion.

With reason, the US and its allies – albeit begrudgingly – moved to exclude Chinese firms from their 5G networks. Not because of corporate malpractice but because of their subjection to China's domestic laws. The contrast with European providers is instructive. Sweden's Ericsson and Finland's Nokia as well as Japanese and Korean component suppliers are also foreign companies but they do not answer to a state that has explicitly made clear its intention to use economic and technological levers against democratic nations.

The 5G decision was relatively clean because 5G is a discrete, identifiable layer of infrastructure with named vendors and clear procurement points. Many of the other technologies that underpin our economies are not like that. The lesson of 5G is not that bans work, but that bans only work when you can clearly identify the layer of concern, enforce the boundary and substitute an alternative. Those conditions don't hold across most of our emerging technology landscape.

Towards a manageable model of technological dependence

We should embark on a more viable pathway towards risk management, one that includes a stratified model of trust. This suggests governments not just articulate security principles but political-economic ones: how they weigh market concentration, supplychain chokepoints, capital ownership, legal jurisdiction and the strategic behaviour of firms and states.

Practically, this means distinguishing between explanatory transparency – clarity about the principles and frameworks governing decisions – and operational discretion – confidentiality about particular cases where disclosure would itself create risk – political, economic or technological. This distinction matters because it allows states to preserve both operational discretion and institutional accountability. Sometimes, governments need to make strategic decisions without publicly disqualifying a specific vendor, system, technology stack or foreign state.

It also means recognising that not all dependencies are equal. Some systems – identity infrastructure, command networks and critical utilities – require tight control and domestic alternatives. Others can tolerate foreign provision if governance, redundancy and oversight are robust.

A stratified model of trust does not resolve the problem of dependence. It clarifies it. It accepts that modern technological systems are structurally interdependent but insists that interdependence can be governed differently depending on its strategic consequences. Trust in this context is not a moral judgment about the intentions of a supplier.

This requires us to engage in the unglamorous work of stack governance: mapping exposure, regulating procurement, shaping markets, investing in alternatives and doing so in coalition with partners who share both vulnerabilities and values.

Foreign ownership of technology is inevitable. Foreign control is not. The path from one to the other runs through the stack, not just through a visible, nameable vendor or product. This leaves us with only one right answer to the question “In Whose Tech We Trust?” That is: in no technology, not without conditions. Trust is a relationship that needs governing. That’s what is critical.

This article is based on two ASPI publications titled “In Whose Tech We Trust”, published in November 2025. Justin Bassi, Executive Director of ASPI, and James Corera, Director of the Cyber, Technology and Security programme at ASPI, also contributed to this article.