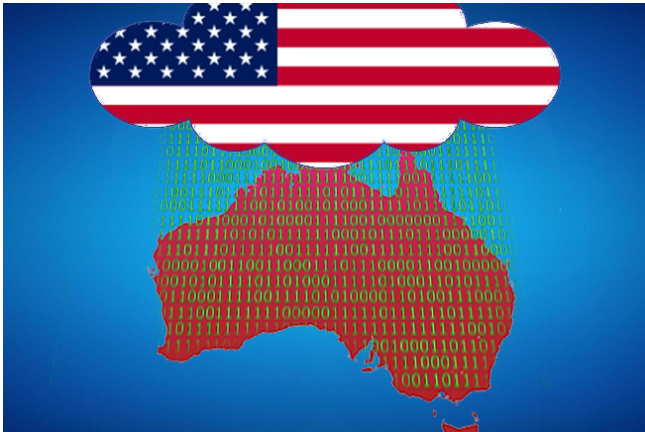


Security without sovereignty: Australia's quiet slide into digital dependency

By Paul Budde

15 October 2025



Australia's deepening digital ties with the U.S. may offer protection — but at the cost of control. [Paul Budde reports.](#)

IN A [PREVIOUS ARTICLE](#), I argued that technological systems created for efficiency were increasingly being repurposed for control. This next chapter extends that concern to the geopolitical level.

Australia's deepening digital integration with the United States, through projects such as the "[Top Secret Cloud](#)", may offer speed and security — but it also risks surrendering sovereignty.

Until recently, few questioned the wisdom of these arrangements. They were presented as pragmatic steps toward faster data sharing and stronger intelligence cooperation. But the world has changed. The United States, once seen as the anchor of liberal democracy, is showing unmistakable signs of authoritarian

drift.

Within a single year, we have witnessed the weaponisation of justice, the erosion of press freedoms and an open contempt for democratic norms. Australia now faces a moral and strategic dilemma: can we trust our most secret systems to a partner that may no longer share our democratic values?

The illusion of secure sovereignty

The cloud project, developed with [Amazon Web Services](#), will host Australia's most sensitive intelligence data inside a privately owned American network. Under the [U.S. CLOUD Act](#), U.S. authorities can legally compel access to data held anywhere in the world. Once our intelligence systems are hosted there, they effectively fall under American jurisdiction.

This is not about whether the United States would misuse that access — it is about the structural error of building a system that allows it. Sovereignty built on trust is not sovereignty at all.

From interoperability to dependency

The "Top Secret Cloud" underpins the [REDSPICE](#) (Resilience – Effects – Defence – SPace – Intelligence – Cyber – Enablers) program, a \$9.9 billion overhaul of the [Australian Signals Directorate](#) designed to make it an AI-driven intelligence agency. It

also supports [AUKUS Pillar II](#), which will integrate Australia's cyber, AI and autonomous systems with U.S. and U.K. capabilities.

What sounds like interoperability in practice becomes dependency. Once decision systems and digital identities are fused across borders, independence is no longer a choice — it's an illusion. We would never host a cloud run by China, yet the moral distance between Washington and Beijing is narrowing fast. Authoritarianism, whether wrapped in nationalism or exceptionalism, remains authoritarianism.

And because this integration proceeds with no serious discussion of sovereignty, Australia risks being locked into America's strategic trajectory, one that could, by design, draw us automatically into a military conflict with China. The technology that ties our systems together could also bind our foreign policy, limiting our capacity to choose neutrality or restraint when tensions rise.

The erosion of transparency at home

Worryingly, this pattern of dependency is mirrored in domestic policy. The [Albanese Government's proposed Freedom of Information reforms](#), framed as a defence against "foreign interference", would make it harder for journalists and citizens to scrutinise decisions. Agencies could reject requests requiring more than 40 hours of work or refuse anonymous submissions.

The timing is striking. As Australia integrates more deeply into U.S.-led defence and intelligence systems, it is simultaneously tightening internal controls over transparency. The less the public can see, the easier it becomes for major strategic decisions – including irreversible technological dependencies – to proceed without democratic consent.

Silence from Canberra

Despite these developments, Australia's political class remains silent. Both major parties cling to the comfort of alliance dependency, unwilling to question whether our security relationship is becoming a form of digital subservience.

The problem is not alliance itself, but the absence of boundaries. Without a clearly defined framework for sovereignty, shared security risks becoming shared obedience. Australia needs to articulate where cooperation ends and control begins — something neither government nor opposition seems prepared to do.

A true alliance between democracies should not require silence. If one partner drifts toward authoritarianism, the other has a duty to resist, not imitate. Our leaders must recognise that the greatest threat to Australian democracy may not come from China, but from blind faith in America's permanence as a liberal power.

Reclaiming sovereignty before it disappears

Security and sovereignty are not the same. Security can be shared; sovereignty must be owned. By outsourcing the architecture of our defence and intelligence systems to a foreign corporation bound by foreign law, Australia risks trading independence for reassurance.

It's time for a national conversation about [technological sovereignty](#) — about what should and should not be embedded within alliance infrastructure. Oversight mechanisms, data firewalls and domestic control must be non-negotiable.

Australia does not stand alone. Strong partnerships remain possible with other stable democracies – in Europe, Canada, New Zealand, Japan and South Korea – nations that continue to uphold transparency, rule of

law and institutional restraint. Broadening our security base through such relationships would strengthen both our independence and our democracy.

Convenience once made us complacent about surveillance. Security may now make us submissive. If we are not vigilant, the cloud that protects us may one day decide for us.

[Paul Budde](#) is an IA columnist and managing director of independent telecommunications research and consultancy [Paul Budde Consulting](#). You can follow Paul on Twitter [@PaulBudde](#).