Who Controls Trust?

As critical systems pass beyond the reach of democratic governments, the sovereignty gap between who is accountable and who is in control is draining trust from the state.



By Andrew Horton
26 October 2026

In the second week of October 2026, two European governments discovered something their citizens had already begun to suspect. Overnight on 11 October, unidentified attackers reached into the refrigeration controllers of between 250 and 350 French supermarkets and set them to defrost. Three days later SpaceX downgraded Ukraine's military-grade Starshield service without warning to Kyiv, and US officials have since told The Wall Street Journal that Elon Musk ordered the slowdown. The details remain disputed. The significance does not. Neither government fell, yet both learned that systems essential to daily life could be altered by actors beyond their control. The disruption mattered. The political message mattered more.

For generations, citizens trusted governments because governments possessed the power to act. States held borders, secured infrastructure, enforced laws and answered crises, and when things went wrong citizens knew who was responsible. That bargain underpins every successful democracy, and it is beginning to weaken. Cloud platforms, satellite constellations, industrial control systems, undersea cables and the infrastructure of artificial intelligence have

become as strategically important as ports, railways and power stations once were, yet governments often control neither their operation nor their continuity. The state keeps the title deeds. Someone else holds the keys.

This is a problem of legitimacy before it is one of cyber security. Governments remain accountable for outcomes they increasingly cannot command. Call it the sovereignty gap: the widening distance between those whom citizens hold responsible for national life and those who possess the practical ability to shape it. The emerging law is unforgiving. When accountability and control part company, trust drains from whoever remains accountable. Citizens may never learn who operates a cloud platform or manages a software supply chain, yet they know whether payments clear, hospitals function and supermarket shelves stay stocked. These are the everyday expectations of state competence.

Most analysts currently believe that as operational power migrates to technology firms and infrastructure providers, public trust will migrate with it. The evidence increasingly suggests that trust is eroding and that the losses fall on government. Concentrated, unaccountable corporate power deepens public unease. It would fail if the new holders of power were inheriting the confidence governments are shedding. Edelman's 2026 barometer points the other way, finding that 54 per cent of low-income respondents expect generative AI to leave them behind, while only 6 per cent of the French expect the next generation to be better off.

> Citizens can forgive governments that fail, but they rarely forgive governments that appear powerless.

Citizens can forgive governments that fail, but they rarely forgive governments that appear powerless. France shows how the verdict forms. The supermarket attacks remain unattributed, with no claim of responsibility and no ransom demand. On 17 October more than 550,000 people marched across France by the interior ministry's count, over wages, schools and the cost of living. The supermarket attacks created none of those grievances. They reinforced something more corrosive, the suspicion that the systems underpinning daily life no longer sit securely within the state's reach. Technology rarely creates political anger. It turns existing frustrations into doubts about who is really in control.

Beijing and Moscow understand this instinctively. In February 2024, Washington, Canberra and their partners warned that Chinese state hackers were pre-positioning inside American critical infrastructure to disrupt it in a crisis or conflict. Authoritarian strategy prioritises leverage over destruction: it seeks to show that the lights could be turned off. Why destroy infrastructure when uncertainty achieves much of the same political effect? Every unexplained outage invites the same question: if the government cannot guarantee

continuity, how much control does it really possess? That question is strategically valuable because it attacks legitimacy itself.

The harder lesson concerns friends. Western governments have spent years reducing their dependence on China across telecommunications, rare earths and advanced manufacturing, and far less examining dependencies embedded in allied technology. The working assumption is that dependence turns benign when the supplier is friendly. Vulnerability is a function of leverage, whatever the intent. Poland, which pays for Ukraine's Starlink subscriptions, had no say over their speed. The compromised French controllers came from an allied Danish supplier whose legacy products no longer received security updates. Dependence on a friend is still dependence.

Australia has already written the test, and applied it in one direction only. In August 2018 Canberra excluded high-risk vendors from 5G on the principle that a supplier likely to be subject to extrajudicial directions from a foreign government that conflict with Australian law could leave a network open to interference. Musk's own account is that the US government sets Starshield's speeds. By the logic of 2018, that is the defining risk. Hostility matters less than whether any external actor holds unilateral authority over systems on which society depends.

Taiwan may grasp this best. After two undersea cables to its Matsu islands were cut in 2023, Taipei trialled low-Earth-orbit satellite backup, and when a cable to the island of Dongyin broke in April 2026, backup links kept its residents connected. Political accountability remains national while operational control increasingly does not, and Taiwan has chosen to narrow the sovereignty gap before Beijing tests it.

The strongest objection is that interdependence is the price of prosperity, and it carries real force. Complete self-sufficiency is neither realistic nor desirable, and Europe's sovereign IRIS² constellation will offer initial services in 2029 at the earliest. Dependence on American capability will remain the price of credible defence for a decade. For three decades advanced economies pursued efficiency above almost everything else, lengthening supply chains and treating resilience as an overhead. Resilience is the foundation of sovereignty, and the strategic competition of this century will reward continuity over scale.

Australia is more exposed than most. Defence halted JP9102, its planned sovereign military satellite system, in November 2024, and the Australian Defence Force has relied on commercial providers and the US Wideband Global SATCOM network. Canberra should legislate an Allied Capability Continuity Standard through the Security of Critical Infrastructure Act and Defence procurement rules, so that every satellite, cloud, software and industrial-control contract supporting defence or essential services carries binding notice before any restriction and a prohibition on unilateral degradation during operations, whatever the supplier's flag. AUKUS partners and the Five Eyes should agree a continuity compact requiring governments to consult before any company in

their jurisdiction degrades a service on which partners depend, and make the identification, disruption and removal of hostile actors from allied networks a shared responsibility.

The sovereignty gap extends well beyond government. Every organisation should know which suppliers retain the power to update, throttle, suspend or disable critical operations, and should regularly test its ability to operate without them. Unsupported connected systems should be removed from public networks. The French supermarket chains learned a simple lesson in a single night: customers blame the empty shelf, not the vendor behind it.

In June 1948, Stalin tried to force a political outcome by controlling the systems that kept West Berlin alive. The airlift prevailed because it restored agency to the people trapped inside the blockade. Trust endured because the West proved it could still act. That is the challenge confronting democracies again. Citizens can tolerate hardship. They can tolerate mistakes. What they will not tolerate indefinitely is powerlessness. The defining political question of the digital age is no longer who governs. It is whether governments still possess the practical power to govern what they are blamed for.