The Private Sector's Increasing Control on National Security

February 8, 2026

For much of the last century, national security was treated as a sovereign stack: intelligence, armed forces, and state-controlled strategic infrastructure. The private sector mattered, but mainly as a supplier.

That separation is thinning across the world. In a period defined by gray-zone pressure, cyber disruption, and sustained geopolitical competition, private firms increasingly operate the systems that keep states functional under stress. They design the networks that move data, the platforms that process it, the factories that scale production, and the services that can be surged in crisis.

This is not a story about governments outsourcing security; states still carry legal authority, coercive power, and strategic responsibility. It is a story about where operational leverage now sits.

Critical Infrastructure and the "Public Risk"

The modern economy runs on privately owned and operated infrastructure that is strategically exposed. Undersea telecommunications cables, which carry the overwhelming majority of transoceanic digital communications, are owned and operated by private companies and consortia. This reality is now being treated as a geopolitical fact, not a technical footnote.

In the **United Kingdom**, this has led to the recognition of the "private ownership of public risk." Under the National

Security and Investment (NSI) Act, the UK government now scrutinizes private acquisitions across 17 sensitive sectors, including AI and energy, treating commercial activity as a core national security vulnerability. Even the UK's nuclear deterrent relies on private firms like Lockheed Martin for maintenance, proving that sovereign capabilities are deeply integrated with private industry.

Similarly, in **Europe**, the NIS2 Directive expands cybersecurity obligations to thousands of private organizations. By making these firms legally responsible for risk management and incident reporting, the EU effectively treats the private sector as the frontline of the "sovereign stack".

The Industrial Base as a Security Instrument

Security competition has returned to a basic question: can capacity be produced fast enough, at scale, and under constraint? This question implicates private industry first. Multi-state security groups now emphasize the need to aggregate demand and use longer-term orders to accelerate industrial capacity.

Australia provides a leading example of building "sovereign capabilities" through private partnerships. To support the AUKUS security partnership, Australia is leaning on private innovation in robotics and quantum technologies. Strategic mergers, such as the Australian firm Penten with the UK-based Amiosec, are now seen as essential to creating global providers of digital security for the state.

Space: A Case Study in Strategic Speed

Space illustrates how commercial services become strategic infrastructure in months, not decades. In recent conflicts, commercial satellite connectivity and sensing became operational necessities. This has triggered a shift in how states like **Canada** view their "digital ambition." Canadian analysts are increasingly arguing for the modernization of the

“sovereign stack” by better integrating private-sector cloud and AI solutions, moving away from rigid, state-only classification frameworks.

Analysis: Future Control and the Security Arithmetic

As we look toward the future, the private sector is fundamentally changing the state’s “security arithmetic”. Private firms do not carry sovereignty, but they carry strategic consequence, creating four recurring dilemmas:

1. **Rule-Setting:** Who sets the rules for access or technical restrictions when private services are used in conflict?
2. **Concentration Risk:** How do states avoid single points of commercial failure without destroying the economics of the private market?
3. **Cross-Border Friction:** How do global firms reconcile operations with sanctions and competing alliance expectations?
4. **Resilience Contracting:** How do governments contract for resilience and “surge capacity” rather than just peacetime performance?

The future of national security will be defined by “dual-use” infrastructure, private runways, ports, and subsea cables that serve both commercial and military purposes. Intelligence is being redefined as private companies become part of “epistemic communities” integrated into state networks due to their specialized data analytics.

A mature approach treats the private sector as a standing component of national security planning. This requires pre-negotiated surge mechanisms, routine exercises that include industry as an operational partner, and the construction of the legal and technical scaffolding necessary to make private capability reliable when the pressure spikes. In a world of persistent competition, the decisive question is no longer just what the state can do, but how effectively it can command

the private leverage it no longer directly owns.

Author: Sohair Saber
Title: Partner – Policy
Email: ssaber@waselandwasel.com
Profile: https://waselandwasel.com/about/sohair-saber/

Lawyers and consultants.
Tier-1 services since 1799.
www.waselandwasel.com
business@waselandwasel.com