DEFENCE & THOUGHT LEADERSHIP

The New Infrastructure of Defence

Sovereignty, technology, and control in a networked world



clearBorder

Opening Manifesto

The ways of working that shaped defence over the last thirty years are being rewritten.

- Capability is distributed
- Supply chains are geopolitical
- Information is strategic
- Technology is harder to govern
- Digital alliances create new forms of dependency
- Sovereignty is conditional
- Control matters more than ownership



This publication explores what those shifts mean – and their implications – for defence leaders.



Christopher Salmon
Chief Executive

FOREWORD

For the last three decades, organisations thought about defence capability, international trade, and geopolitical risk as largely separate conversations. Today, they are inseparable.

Questions that once sat within procurement, compliance, engineering, or government affairs now reach the boardroom. Decisions about suppliers, technology, investment, data, partnerships, and export controls now shape not only commercial performance, but an organisation's long-term strategic freedom.

At clearBorder, we work with organisations as these pressures continue to evolve. And, while every organisation works within its own circumstances, the strategic questions are consistent.

This publication brings those conversations together. Throughout these pages, I, along with my colleagues Ian Hunt and Sarah Rice, explore how capability is becoming increasingly digital, distributed, and connected – and what that means for organisations responsible for building, protecting, and governing it.

One recurring message is this: competitive advantage and organisational growth belongs to those that understand not only where capability resides today, but where control over that capability will sit tomorrow.

Further insight

clearBorder supports defence organisations, manufacturers, investors, and executive teams in navigating complex international trade. Explore more of our latest defence insights, executive resources, and board-level perspectives.

Defence →

For the Boardroom →

Executive Overview

The five shifts redefining defence

1

Capability is distributed

Military capability resides across complex networks of manufacturers, software providers, engineering partners, and specialist suppliers. Strategic advantage depends on understanding and governing that ecosystem.

2

Supply chains are geopolitical

Governments view supplier ecosystems, operational dependencies, and industrial resilience as matters of national capability. Supply chains have become strategic infrastructure.

3

Information is strategic

Engineering expertise, software, technical data, AI, and digital know-how determine strategic advantage. Knowledge is as important to capability as physical hardware.

4

Digital alliances create capability and dependency

Modern defence depends on trust and digital collaboration across governments, industry, and allies. Every new connection strengthens capability while introducing new strategic dependencies.

5

5. Control matters more than ownership

Ownership does not guarantee operational freedom. Strong governance enables organisations to move faster, collaborate confidently, and preserve greater strategic freedom as geopolitical conditions evolve.



Sovereignty

Ownership matters less than control.

Christopher Salmon leads clearBorder's strategic advisory work, helping organisations navigate the intersection of international trade, sovereign capability, geopolitics, and border policy. He is a former adviser to UK Cabinet Ministers on customs, export controls, and defence-related trade during the UK's departure from the EU and brings first-hand insight into how governments think about strategic capability, resilience, and control.



Christopher Salmon
Chief Executive

Capability is not sovereignty

A conversation on control, cost, and credibility in defence

KEY INSIGHTS

1 **Boardrooms should treat sovereign capability as a question of operational control. Capability exists on a spectrum.** The more organisations understand where permissions, dependencies and external constraints exist, the greater their freedom of action becomes.

2 **Sovereignty is shaped by governance.** Export controls, licensing regimes, supply chains and industrial capacity now influence commercial resilience as much as technical capability.

3 **Strong organisations manage sovereignty rather than assume it.** They invest in foresight, understand where dependencies exist, and continually assess how geopolitical change could affect their ability to operate, innovate and grow.





Sovereign capability is politically compelling. Operationally, it is considerably more complicated.

As a phrase, sovereign capability is gaining significant attention across defence and policy circles. Christopher Salmon has spent years working at the intersection of defence, regulation and procurement, and believes the concept is often misunderstood.

"It is a bit of a buzzword," he says candidly. *"But the central concept isn't new. What's changed is the context. We're no longer thinking in a post-war environment. Increasingly, people are thinking in pre-war terms. That changes how seriously you take questions of control."*

At first glance, sovereign capability appears straightforward.

"It's the technology you can use," Christopher explains, *"without being restricted by somebody else."*

For aerospace, defence and manufacturing leaders, however, that simplicity rarely survives contact with reality.

The sovereignty paradox

"Sovereign capability is not an absolute concept," Christopher says. *"You're not either sovereign capable or not sovereign capable. The more of the chain you control, the better. But you're never going to control all of it."*

It is an observation that sits at the heart of modern defence. Organisations can own platforms, manufacture systems and deploy sophisticated capability. Yet they may still require external permission to modify software, transfer technology, export products or integrate new components.

Ownership, in other words, does not always confer operational freedom.

This is the sovereignty paradox. *"You can own a system,"* Christopher explains, *"you can operate it, you can deploy it. But if there are restrictions on how you use it, modify it or transfer it, then your sovereignty is already conditional."*

Programmes such as AUKUS demonstrate this clearly. Alliances can deliver extraordinary capability while simultaneously embedding layers of shared governance, regulatory oversight and partner dependency.

That is not necessarily a weakness. It is the architecture of modern defence.

"There has always been a desire for states to control their advantage," Christopher says. *"What changes is what counts as strategic — and who controls it.*

"It doesn't matter how clever your system is if you can't produce it at scale. If you've only got a million shells and you're firing a million a week, you've got a problem very quickly."

Industrial capacity, supply chains and manufacturing resilience remain as important to sovereignty as cutting-edge technology.

The governance behind capability

People often picture sovereign capability in terms of ships, aircraft or advanced weapons. Christopher sees something different.

"People often think of sovereign capability in terms of hardware. In practice, it's governed by legal and regulatory frameworks just as much as anything else."

Export controls, licensing regimes, sanctions and national security legislation define what organisations are able to do. Frameworks such as ITAR extend influence well beyond national borders.

"You can buy something, integrate it, make it part of your system," Christopher says. *"But if it's subject to external control, then the permission structure doesn't sit with you."*

The UK's National Security and Investment Act reinforces the same principle by bringing ownership, investment and strategic capability under closer government scrutiny.

Capability therefore becomes as much a governance challenge as a technical one. For smaller businesses, this often manifests as uncertainty.

"They know they're dealing with something sensitive," Christopher explains. *"Maybe it's dual-use, maybe it's regulated. But they don't always have the infrastructure to manage that properly."*

For larger organisations the question becomes more strategic.

"Do we build around something that gives us capability now, but constrains us later? Or do we invest in something that gives us greater freedom of action over the long term?"

That is no longer simply a compliance decision. It is a boardroom decision.

"You can buy something, integrate it, make it part of your system," Christopher says. *"But if it's subject to external control, then the permission structure doesn't sit with you."*

The cost that rarely appears on the balance sheet

The true cost of sovereign capability is rarely paid upfront. *"Organisations will model the upfront cost,"* Christopher says. *"They won't always model the downstream constraints."* Those constraints emerge later:

- When products cannot be exported.
- When technologies cannot be transferred.
- When suppliers become politically unavailable.
- When permissions change.
- Control lists evolve.
- Sanctions shift.
- Critical components suddenly become difficult to source.

"If you're reliant on a particular component, or a particular material, or a particular jurisdiction," Christopher says, *"then you are exposed. Whether you planned for that or not."*

By the time those dependencies become visible, they are often deeply embedded. *"The market will find alternatives,"* he says. *"But it won't be quick. And it won't be cheap."*

What the strongest organisations do differently

Christopher believes the organisations navigating this environment most successfully share a common characteristic. They plan before circumstances force them to react. *"The first thing is foresight,"* he says. *"You have to look ahead. You can't just react."*

For decades, geopolitical risk sat quietly in the background while businesses focused on technology, efficiency and growth. That balance has shifted.

"Politics is now a much bigger part of business decision-making." Consequently, supply chains, compliance, regulation and geopolitical exposure have become core operational disciplines rather than specialist concerns.

"You manage your finances carefully," Christopher says. *"You need to manage your international supply chains in the same way. It's more important to make sure they can hold up under pressure."*

Above all, organisations must become comfortable managing uncertainty. *"Doubt and ambiguity are part of the international system now,"* he says. *"You have to plan for it."*

Sovereignty as a managed condition

The conversation around sovereign capability will only become more important. But it also needs to become more realistic.

"There is no country in the world that doesn't need to trade," Christopher says. *"You're always going to be dependent on something."* True sovereignty, therefore, is rarely absolute.

It is built gradually through visibility, resilience, governance and deliberate choices about where organisations are willing to accept dependency.

"Essentially, it's about how much of the chain you control," Christopher says. *"And what that allows you to do."* For today's leadership teams, that means asking questions like:

- Where are we constrained?
- Where are we exposed?
- Where does control actually sit?



Because sovereign capability is no longer something organisations can simply claim. It is something they must continuously earn, strengthen, and manage. As Christopher puts it: ***"the more of it you can genuinely hold onto... the better."***

Executive Briefing 01

Europe's defence sovereignty



BOARDROOM CONSIDERATION

Is your supply chain optimised for efficiency – or trusted resilience?

Europe's push for defence sovereignty is reshaping supply chains, industrial policy, export controls, and the way governments assess trusted capability. Organisations compete on resilience as well as technology, meaning supplier transparency, allied-country sourcing, and governance are commercial differentiators. As capability becomes more distributed and software-defined, businesses must be able to demonstrate not only what they build, but where critical components, knowledge, and dependencies reside across their ecosystem.

Read the full article

Executive Briefing 02

AUKUS and conditional capability

AUKUS illustrates how modern alliances operate through shared governance as much as shared capability. While collaboration expands military strength, it can also embed regulatory dependence through licensing, export controls, and policy alignment. Capability may be nationally owned while remaining operationally constrained. Therefore, sovereignty depends not simply on possessing capability, but understanding the permissions, obligations, and strategic conditions that govern its use.

"Capability does not always equal autonomy.

Ownership does not always equal control."



Read the full article

Executive Briefing 03

Strategic capability is distributed



Modern defence capability is spread across specialist manufacturers, software companies, engineering consultancies, cloud providers, AI developers, and highly specialised subcontractors. As governments focus more closely on industrial resilience, understanding where critical capability resides has become a strategic leadership responsibility.

"The question is not who builds the platform, but who makes the platform possible?"

Read the full article

Systems

Capability becomes operational when the systems behind it can support it.

Ian Hunt is one of clearBorder's export control specialists, helping organisations across aerospace and defence build practical governance around ITAR, licensing, technical data, and international collaboration. Having worked both inside major defence programmes and alongside government, he understands how export control sits within engineering, operations, and digital systems.



Ian Hunt
Trade Control Consultant

ITAR in the age of automation

Why export control is a governance challenge

KEY INSIGHTS

1 **Export control depends on how information moves through an organisation.** As defence capability becomes more digital, compliance is shifting closer to engineering, software, cloud infrastructure, and operational decision-making.

2 **Automation strengthens governance only when the underlying information is accurate.** AI and automated workflows improve traceability, consistency, and auditability, but they cannot compensate for weak governance or poor-quality data.

3 **Future-proof firms embed compliance into the way they operate.** They build governance into engineering, programme management, technology architecture, and day-to-day business systems.



The biggest risk with ITAR isn't a missing licence. It's losing control of information.

Some defence organisations still treat ITAR as a licensing exercise, while regulators treat it as a governance issue. As businesses digitise operations, automate workflows, adopt AI-enabled systems, and manage growing volumes of technical data, export control sits inside the architecture of the organisation itself.

The challenge is governing how information moves through systems, teams, suppliers, and international programmes.

"The future of ITAR compliance will be determined less by who files the licence, and more by how organisations govern the data, systems, and information flows behind it."



The consequences of failure have changed

Civil penalties can exceed $1m per violation, organisations can lose export privileges, suffer reputational damage, or find themselves excluded from critical defence programmes.

In extreme cases, individuals can face personal liability and criminal prosecution.

"Export control failures don't become business problems overnight. They creep in through weak governance, poor visibility, and unchallenged assumptions."

Ian Hunt, export controls specialist at clearBorder, states that it wouldn't be unusual to work with a company undergoing regulatory review where the issue wasn't a lack of expertise, or intent, but **visibility**.

The information can exist, but if it's fragmented across spreadsheets, folders, and disconnected systems – when regulators ask questions – the organisation will struggle to demonstrate control.

ITAR has become a systems challenge

Major defence organisations have spent years embedding compliance directly into their operational infrastructure; from document controls and access permissions to transfer approvals, metadata tagging, and information management systems.

The objective? **To make compliance part of the workflow**, rather than a final-stage intervention.

A decade ago, export control relied largely on manual processes, spreadsheets, and individual expertise; a model that has become difficult to sustain. Ian has seen this evolution first-hand.

For smaller organisations, the challenge is particularly acute. While large defence primes have invested aggressively in embedding and automating governance environments, many SMEs and fast-growth businesses still rely on spreadsheets, fragmented processes, and individual expertise.

Regulators expect both to demonstrate the same level of control.

> *"Historically, organisations treated export control as something that happened at the point of shipment. Today, the strongest organisations build compliance directly into how information is created, stored, accessed, transferred, and managed."*



Automation raises the bar for governance

It's tempting to view automation as a compliance solution in its own right. That is a mistake. Properly deployed, automation strengthens traceability, creates auditability, enforces controls, and makes governance more scalable.

It cannot compensate for weak data, poor governance, or unclear ownership.

"The data out is only as good as the data in."

That is the crux of the modern compliance challenge.

Every automated control system ultimately depends on the quality of the information feeding it. Incorrect classifications, incomplete supplier information, weak record-keeping, or poorly maintained data structures will simply produce automated versions of the same problems.

AI may help classify products, prepare applications, flag anomalies, and support screening activity. But responsibility remains human. Automation can accelerate decision-making. It cannot own it.

In the eyes of regulators, *"that's what the system says"* is not a defence. Organisations remain responsible for:

- How systems are configured
- How decisions are made
- Whether governance controls are operating effectively

"You can automate compliance tasks. You cannot automate accountability."

Compliance sits closer to engineering and operations

As software, technical data, digital twins, cloud environments, and globally distributed engineering teams become more common, compliance decisions need to be made at the beginning of activity.

Historically, compliance usually appeared near the end of a process. Products were designed; supply chains were established; programmes were launched; compliance teams were then asked to validate what had already been built.

In the modern era, export control sits much closer to:

- Engineering design
- Product development
- Technology architecture
- Supply chain planning
- Data governance
- Programme management

"Compliance cannot be an end-stage activity. It has to be present from the outset."

"The biggest mistake organisations make is treating compliance as something to address later. By then, most of the important decisions have already been made."



Record-keeping as a strategic capability

Regulatory investigations repeatedly expose the same weakness: poor record-keeping.

If approvals cannot be found, decisions cannot be traced, or data cannot be verified, regulators are unlikely to accept assurances that processes were followed correctly.

Automation plays a role here because it creates traceability. Time-stamped records, auditable workflows, approval histories, and system-generated evidence can all strengthen an organisation's ability to demonstrate control.

"If you don't have a record of it, it didn't happen."



The bigger picture

Much of the conversation around sovereign capability focuses on industrial capacity, shipyards, manufacturing facilities, and weapons production. ITAR itself was originally designed to control the movement of physical defence articles.

Now, its challenge is controlling the movement of information. As defence capability becomes increasingly digital, ideas of sovereignty must expand to include information itself; *information* such as:

- Technical drawings
- Engineering models
- Source code and encrypted software
- Controlled datasets
- Digital twins
- Sensitive programme information

These assets now sit at the heart of military capability.

The question is not whether organisations adopt automation. They will. The question is whether corporate governance matures at the same pace. Because – while automation will make good governance stronger – it will only make weak governance more dangerous.



"As defence becomes more digital, information is capability. Controlling information matters as much as controlling hardware."

Executive Briefing 04

National security starts early



BOARDROOM CONSIDERATION

Which commercial decisions being made today could become tomorrow's national security questions?

The National Security and Investment Act reflects a broader change in how governments assess strategic industries. National security risk develops through procurement, supplier relationships, investment decisions, technology partnerships, and access to critical capability long before regulators become involved. Organisations that identify these issues early protect commercial opportunities while reducing regulatory friction.

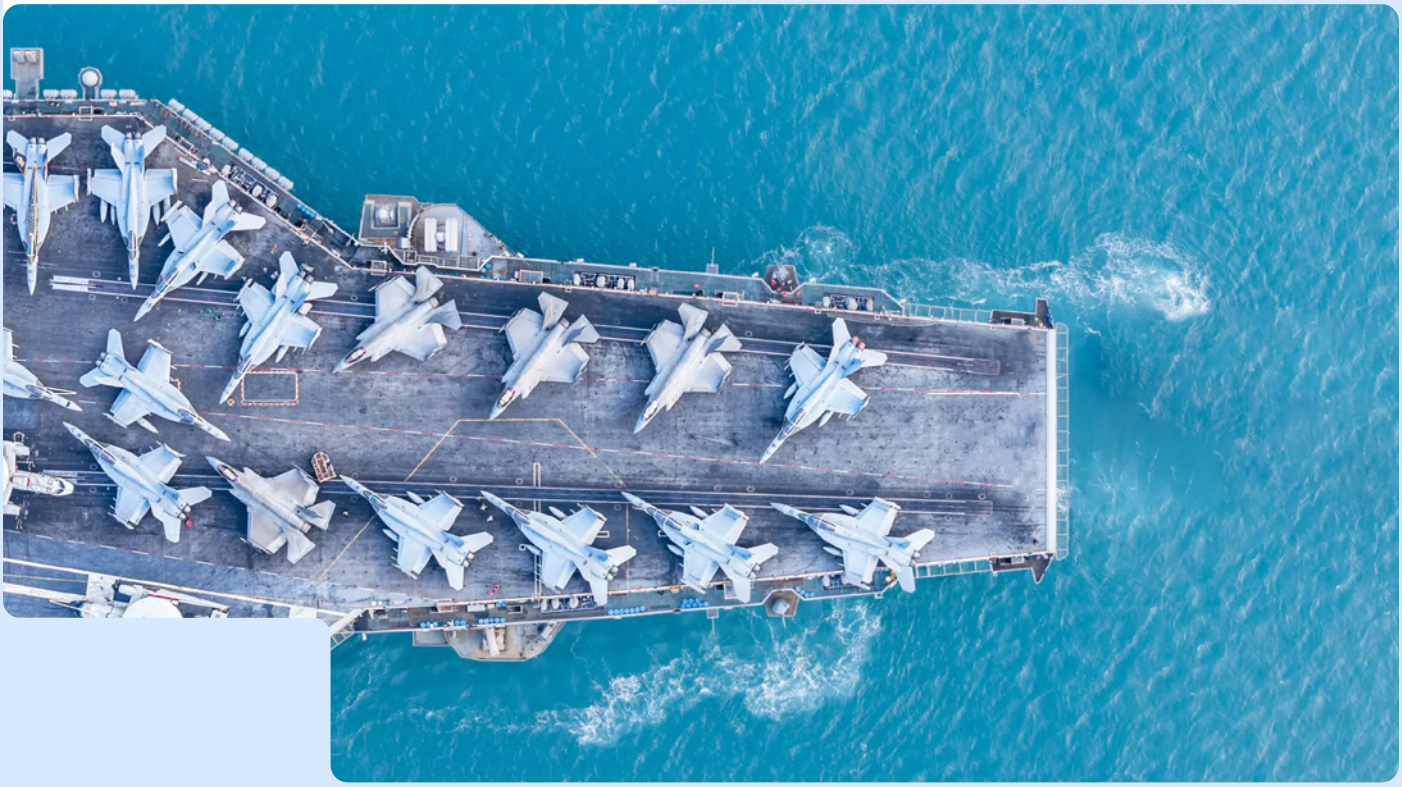
Read the full article

Executive Briefing 05

Investment is geopolitical

Foreign investment brings questions of influence alongside questions of finance. Governments assess who funds, accesses, and shapes strategically important capability as carefully as they assess the capital itself. Investor due diligence is therefore an exercise in strategic resilience as much as corporate finance. Being able to demonstrate transparent governance and trusted ownership structures will find investment easier to secure – and easier to defend.

> *"Capital doesn't just buy equity. It can also buy influence."*



Read the full article

BOARDROOM CONSIDERATION

Would regulators view your next investor through the same lens as your board?

Knowledge

Modern defence depends on controlling knowledge – not hardware.

Sarah Rice leads clearBorder's export control consultancy, advising organisations across defence, aerospace, photonics, quantum, space, and advanced manufacturing. With more than 25 years' experience spanning ITAR, dual-use goods, sanctions, licensing, and international trade, she helps organisations build governance that protects sensitive capability while enabling confident international collaboration.



Sarah Rice
Head of Export Controls

Technology transfers in a controlled world

KEY INSIGHTS

1 **Knowledge is a strategic asset requiring strong governance.** Engineering expertise, software, AI models, technical data, and digital know-how underpin sovereign capability – making control over knowledge as important as control over products.

2 **Businesses must understand where knowledge resides, who can access it, and how it moves across organisational and national boundaries.** Modern technology transfers involve digital information, meaning collaboration, cloud platforms, engineering environments, and data sharing all carry export control implications.

3 **The value lies in governing knowledge without restricting innovation.** By embedding visibility, clear decision-making, and proportionate governance into international collaboration, firms protect sensitive capability while continuing to innovate, partner, and grow with confidence.



> *"It's not that the rules themselves have changed. But everything else has."*

According to Sarah Rice, clearBorder's Head of Export Controls, that observation encapsulates much of today's export landscape.

Physical technology transfers remain a core part of international trade: defence equipment, engines, sensors, drones, components, and other controlled goods continue to move across borders every day. Increasingly though, some of the most valuable defence capabilities never touch a shipping container at all.

They move through engineering software, CAD models, the cloud, remote meetings, source code, digital twins, AI systems, technical data, and collaborative research.

"The most valuable exports of the modern defence era never pass through a customs checkpoint."

The challenge for firms? It's not only controlling *where* products go. It's more about understanding where the knowledge lives.

Invisible exports

Twenty years ago, export controls largely centred on physical goods. Today, organisations also need to think about **invisible exports**: software, engineering models, CAD files, cloud platforms, source code, technical data, automated systems, and even conversations that reveal controlled capability.

That has fundamentally changed the nature of technology transfer.

Many organisations underestimate just how easily technology can cross borders. A controlled export might now involve:

- Sharing a CAD drawing during a Teams meeting
- Providing code to a development partner
- Allowing an overseas visitor into an engineering design review
- Going on holiday with technical data stored on a laptop
- Granting access to cloud-based environments

"Tomorrow's export controls will be defined by who gains access."



The geography of knowledge

Governments have always been interested in where strategic capability is manufactured. These days, they are interested in where it resides.

The reason is straightforward: **controlling access to knowledge means controlling future capability**. Whoever possesses the expertise, software, data, or AI models will ultimately possess the strategic advantage.

- *Who can access it?*
- *Who can copy it?*
- *Who can build upon it?*
- *Who ultimately benefits from it?*

For Sarah, this reflects a broader geopolitical shift.

"Countries are working harder to keep strategically important technologies 'in the family', while applying greater scrutiny where knowledge might flow beyond those networks."

That helps explain why defence cooperation agreements like AUKUS have become so important. More than just accelerating collaboration, the objective is to enable it within frameworks and alliances of trust that protect confidence over how sensitive capability is shared.

Regulators are following the knowledge

Three recent enforcements illustrate this. Each is different in its detail, but together, they reveal a clear direction of travel.

- **General Electric** accepted a $36 million penalty from the US State Department after more than one hundred ITAR violations involving military engines, including data associated with the F-35. The case centred on failures to govern engineering information, licensing, digital systems, and employee handling of controlled data.
- **RTX** agreed to a $200 million administrative settlement following hundreds of export control violations involving engineering data, foreign national employees, laptops, and technical information relating to some of the United States' most sensitive defence platforms. Again, the issue here was systemic governance, not the movement of finished products.
- Temporary US restrictions on access to **Anthropic's most advanced AI** models demonstrate that governments are thinking differently about frontier capability itself. The essence of the debate was around access to models that will likely underpin future economic and military advantage.



"Governments are regulating the know-how behind the product. Not just the product itself."

Regulators are looking beyond physical exports – it's not "what left the country?", but "who gained access?"

Collaboration without paralysis

None of this means organisations should become reluctant to innovate. Research partnerships, international engineering teams, universities, suppliers, and global collaboration remain fundamental to progress.

The challenge is building governance that protects sensitive capability without discouraging legitimate collaboration. For innovative businesses, the objective must be to understand what can be shared, with whom, and under what conditions.

- *Do you know what controlled information you hold?*
- *Can you identify when technology transfers are taking place?*
- *Who has access to sensitive engineering data?*
- *Can you demonstrate why certain decisions were made?*
- *Have you documented your reasoning?*

> *"Technology transfer becomes manageable the moment you recognise it's happening."*

Perhaps the biggest misconception is that compliance inevitably slows innovation. In reality, organisations with mature governance collaborate more confidently because they understand what can be shared, what cannot, and where appropriate licences or exemptions already exist.

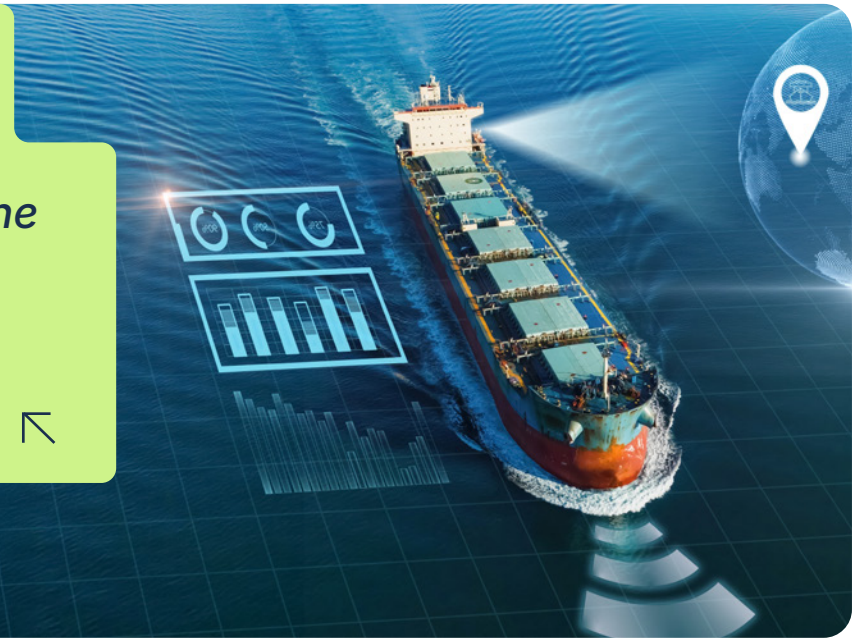
A new era of technology transfers

Technology transfer has always been about capability; what's changed is the form that capability can take.

For governments, that means looking beyond factories and freight routes towards software, engineering knowledge, AI models, technical data, and the increasingly digital foundations of national capability.

That changes how policymakers think about sovereignty, how regulators enforce export controls, and how businesses should manage innovation, partnerships, and international growth.

> *"The winners won't be those that share less knowledge. They'll be the firms that know exactly what they're sharing, with whom, and why."*

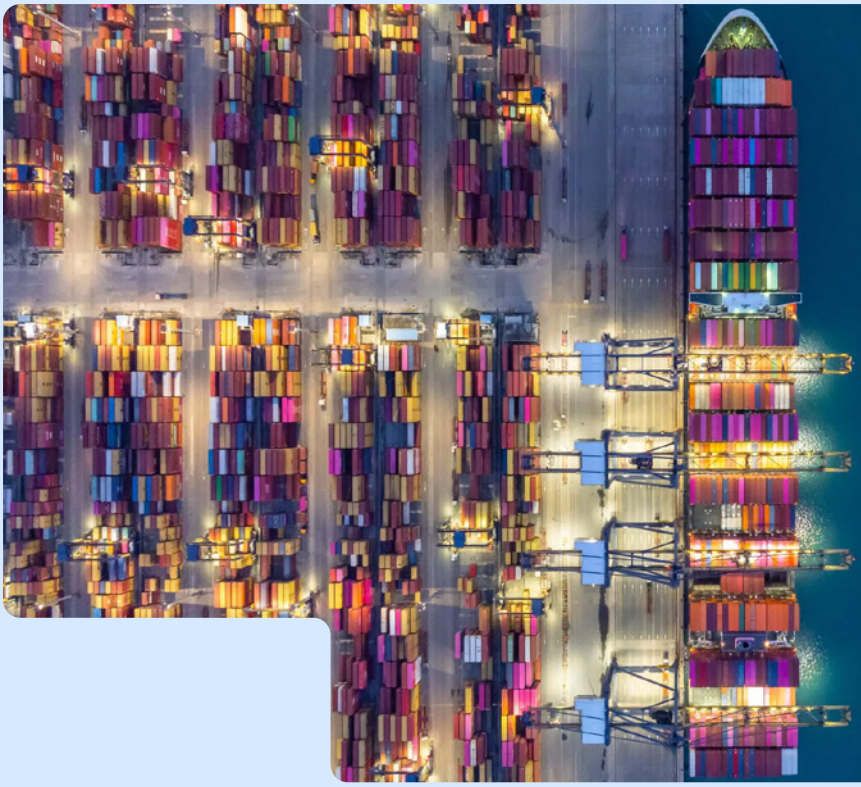


As technology becomes more digital, the advantage will belong to organisations that can innovate freely and collaborate confidently while still maintaining control over where the knowledge behind that innovation lives.

Executive Briefing 06

Diversification changes risk

Diversification does not guarantee resilience. Every new supplier, market, programme, or international partnership redraws an organisation's regulatory perimeter, introducing fresh export control, licensing, sanctions, and technology transfer considerations. The organisations that expand successfully are those that understand the regulatory consequences of growth before committing capital or capability, creating a governance dividend.



"The governance dividend is the freedom to grow without losing control of the business you are building."

Read the full article

Executive Briefing 07

Alliance fabric



BOARDROOM CONSIDERATION

Do your digital partnerships strengthen your strategic freedom or create dependencies you have yet to recognise?

Modern capability depends on trusted digital relationships. Data sharing, cloud infrastructure, AI, engineering environments, and secure collaboration underpin programmes such as AUKUS Pillar II, NATO interoperability initiatives, and multinational defence partnerships. The resulting alliance fabric allows capability to move confidently between governments, industry, and allies – but every new digital connection creates new strategic dependencies that leadership teams must understand and govern.

Read the full article

Farnborough Intelligence

Strategic signals from Farnborough Airshow 2026

One of the most significant discussions at **Farnborough International Airshow** was around the shift in how governments, defence companies, and allies think about sovereignty. Ultimately, competitive advantage depends on **the systems that underpin capability**: systems including governance, industrial resilience, trusted partnerships, and operational control.

1 **Sovereignty is a procurement requirement.**

Governments want local production, technology access, and greater freedom to maintain and adapt critical capability. For businesses, advantage depends on demonstrating control, resilience, and long-term industrial participation.

2 **Affordable mass is a strategic advantage.**

Scalable production was a recurring theme at the show. Cost per engagement matters as much as technical performance – and so manufacturing capacity, production resilience, and unit economics are now core strategic capabilities.

3 **Autonomy enters the operational mainstream**

Collaborative aircraft, autonomous logistics, and AI-enabled systems are integral to future force design. Success, therefore, requires greater emphasis on software assurance, interoperability, data governance, and system integration.

4 **Alliances are industrial ecosystems.**

Cross-border collaborations show that modern alliances need shared industrial capability. Partnerships should be evaluated as long-term operating models, with governance, technology access, and decision rights clarified early.

5 **Industrial capacity is capability.**

Demand remains strong, but production constraints continue to shape delivery, procurement, and operational readiness. Supply chain visibility, manufacturing resilience, and supplier governance are sources of competitive advantage.

6 **Defence spending is industrial policy.**

Governments expect investment to deliver broad economic value. Therefore, organisations should strengthen the commercial case for domestic investment, skills development, innovation, and long-term industrial contribution.

7 **Resilience depends on connected systems.**

True resilience is created by the networks that connect assets. Executive oversight should encompass suppliers, data, technology dependencies, and trusted partnerships.

The language of modern defence

The sovereignty paradox
Ownership of capability does not necessarily confer operational freedom. An organisation may own a platform, technology, or system while remaining constrained by export controls, licensing conditions, alliance commitments, or regulatory permissions.

The governance dividend
The commercial advantage created when governance enables strategic freedom rather than constraining it.

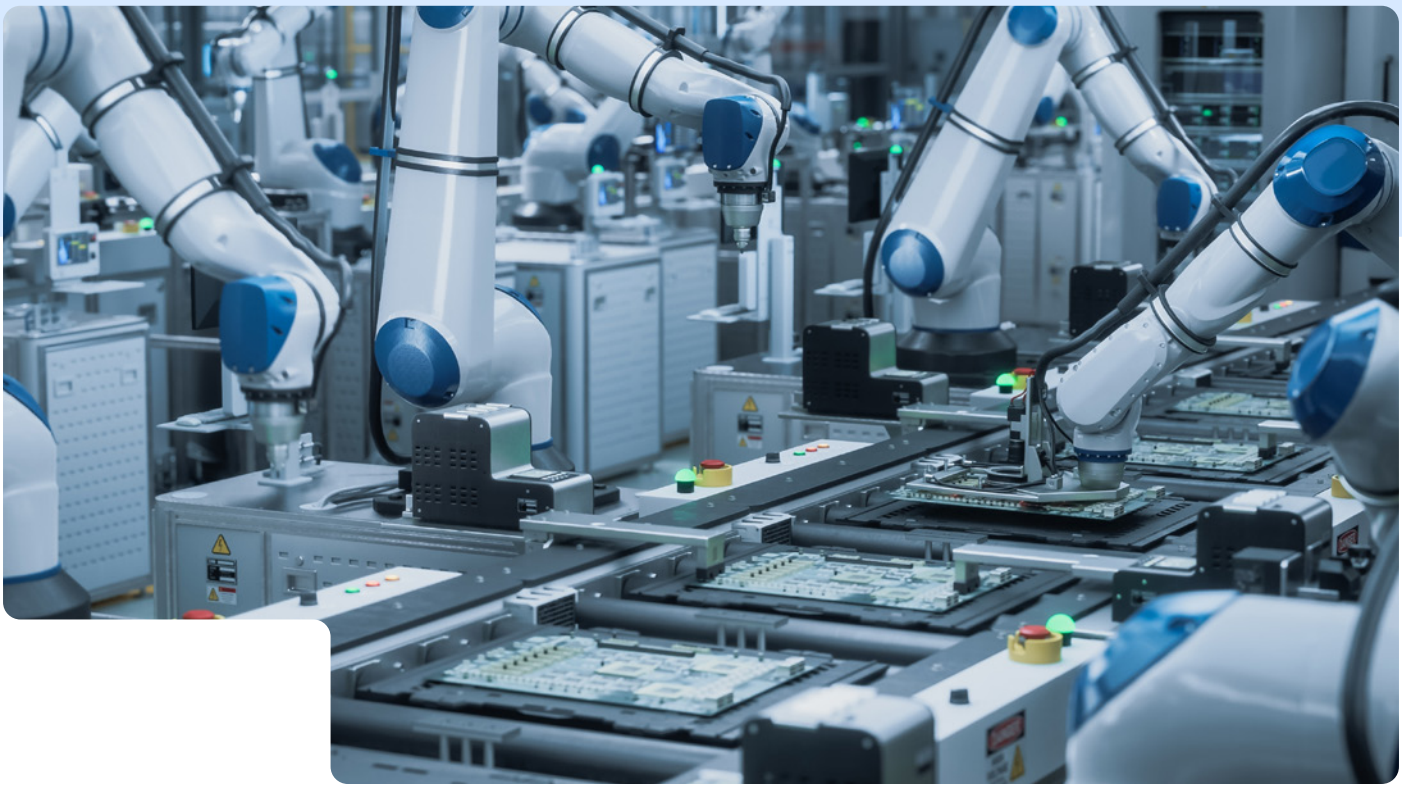
Regulatory perimeter
The expanding boundary of regulatory obligations created by every new supplier, market, technology, programme, or international partnership.

Alliance fabric
The weave of trusted digital relationships that enables governments, organisations, industry partners, and allies to exchange capability securely across organisational and national boundaries.

Capability gravity
The tendency for strategically important capability to accumulate around organisations upon which large parts of the defence industrial ecosystem depend.

The geography of knowledge
The distribution of strategically important expertise, engineering knowledge, software, technical data, AI, and intellectual property across organisations, systems, and jurisdictions.

Connected capability
Military capability created collectively through networks of organisations, software, engineering environments, cloud infrastructure, and shared information.



Final thoughts

The view beyond Farnborough



Christopher Salmon
Chief Executive

Farnborough Airshow is about more than new planes and aerospace technologies; it's also about policy, procurement, and industrial strategy. While there's always something extraordinary about standing beneath the aircraft and seeing the engineering up close, what was most valuable was catching up with those whose work turns ambitious ideas into operational capability. My thanks to everyone who made time to share their perspectives.

Everything we saw and heard reaffirmed that – beyond individual assets or platforms – modern defence is built through infrastructure; those connected networks of supply chains, secure information, industrial capacity, trusted alliances, and governance that preserves freedom of action.

The UK's Defence Investment Plan commits £298 billion over the next four years, including significant investment in autonomous systems, munitions, and next-generation air capability. The task now? It is one of delivery: turning intent into scalable production, enduring partnerships, and true operational readiness.

That said, the Plan was formalised under the UK government's previous leadership. With Andy Burnham now in Downing Street, and promising to use public procurement to reindustrialise Britain, it'll be interesting to see how the agenda evolves.

> *Indeed, these are changing times, and there is more geopolitical uncertainty on the horizon. But for organisations prepared to understand and govern* ***the new infrastructure of defence****, these are also times of considerable opportunity.*

Continue exploring

Borders for the Boardroom

Our podcast explores the forces reshaping international trade, defence, geopolitics, export controls and global supply chains.

Listen now on Spotify and Apple Music

Defence

The latest analysis covering sovereign capability, export controls, industrial resilience, defence procurement, geopolitics, and the evolving defence landscape.

Visit our Defence hub →

For the Boardroom

Practical insights created for executives navigating complex international trade.

Visit our Boardroom hub →

Case Studies

See how we help organisations reduce risk, unlock opportunity, strengthen governance, and build long-term resilience.

Explore our client case studies →

How we help

Governance

Build governance frameworks that strengthen resilience, improve accountability, and embed compliance into everyday decision-making.

Export Controls

Navigate UK, EU and US export control regimes with practical advice on licensing, military goods, dual-use products, technology transfers and compliance.

Customs & International Trade

Reduce friction across borders through practical customs strategy, compliance support and operational guidance.

Strategy & Horizon Scanning

Anticipate regulatory change, geopolitical developments and emerging trade risks before they become operational challenges.

Complex & Regulated Goods

Specialist support for organisations trading sensitive, regulated, or strategically important products across international markets.

Explore all our services →

Meet our team →

Continue the conversation

Whether you're preparing for international expansion, reviewing supply chain resilience, navigating exports or strengthening governance – we're here to help you make informed decisions with confidence, clarity, and control.

Contact the clearBorder team →

The new infrastructure of defence



Control is more valuable than ownership.

Capability depends on connection.

Governance is competitive advantage.

Get in touch: info@clearborder | clearBorder.co.uk

clearBorder

Helping organisations navigate the future of international trade.